TENDER DOCUMENT GOODS AND SERVICES	CITY OF CAPE TOWN ISIXEKO SASEKAPA STAD KAAPSTAD
SUPPLY CHAIN MANAGEMENT	
SCM - 542 Approved by Branch Manager: 03/04/2020	Version: 8 Page 1 of 284

TWO STAGE TENDER

TENDER NO: **41S/2022/23**

TENDER DESCRIPTION: **SUPPLY, INSTALLATION, SERVICE AND MAINTENANCE OF A RECORDS MANAGEMENT DOCUMENT MANANGEMENT AND CASE MANAGEMENT (RM&DM&CM) SOLUTION FOR THE CITY OF CAPE TOWN**

CONTRACT PERIOD: **FROM DATE OF COMMENCEMENT OF CONTRACT UNTIL 31 MAY 2033**

VOLUME 1: TENDERING PROCEDURES

CLOSING DATE: **9 SEPTEMBER 2022**

CLOSING TIME: **10:00 a.m.**

TENDER BOX
NUMBER: **156**

TENDER FEE: R200.00 Non-refundable tender fee payable to City of Cape Town (CCT) for a hard copy of the tender document. This fee is not applicable to website downloads of the tender document.

TENDERER	
NAME of Company/Close Corporation or Partnership / Joint Venture/ Consortium or Sole Proprietor /Individual	
TRADING AS (if different from above)	

NATURE OF TENDER OFFER (please indicate below)	
Main Offer (see clause 2.2.11.1)	
Alternative Offer (see clause 2.2.11.1)	

TENDER SERIAL NO.:	
SIGNATURES OF CITY OFFICIALS AT TENDER OPENING	
1	
2	
3	

TABLE OF CONTENTS

VOLUME 1: THE TENDER
(1) GENERAL TENDER INFORMATION

TENDER ADVERTISED	:	**22 JULY 2022**

CLARIFICATION MEETING	:	10h00 on 10 August 2022
		(Compulsory)
VENUE FOR CLARIFICATION MEETING	**:**	Banqueting Hall, 5th Floor Podium Block, Civic Centre as well as via Skype on the link below: **https://meet.capetown.gov.za/fabiaetumeleng.sekese/6CYDBNW2**

TENDER BOX & ADDRESS	:	**Tender Box as per front cover** at the **Tender &Quotation Boxes Office**, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town. The Tender Document (which includes the Form of Offer and Acceptance) completed in all respects, plus any additional supporting documents required, must be submitted in a sealed envelope with the name and address of the tenderer, the endorsement "**TENDER NO. DP5522S/2019/20 - SUPPLY, COMMISSION, INSTALLATION, SERVICE AND MAINTENANCE OF AN RM&DM&CM SOLUTION TO THE REQUIREMENT OF THE CITY OF CAPE TOWN.** The tender box No. and the closing date indicated on the envelope. The sealed envelope must be inserted into the appropriate official tender box before closing time.
		If the tender offer is too large to fit into the abovementioned box or the box is full, please enquire at the public counter (Tender Distribution Office) for alternative instructions. It remains the tenderer's responsibility to ensure that the tender is placed in either the original box or as alternatively instructed.

CCT TENDER REPRESENTATIVE		Email: CAR.Tenders@capetown.gov.za

TENDERS ARE REQUESTED TO ALWAYS REFERENCE THE TENDER NUMBER IN ALL COMMUNICATIONS FOR THIS TENDER

The Employer's Information Officer who is responsible for overseeing questions in relation to data protection may be contacted at Popia@capetown.gov.za.

By submitting a tender to the City of Cape Town, (and by concluding any ensuing related agreement with the City of Cape Town, if applicable), the Tenderer thereby acknowledges and unconditionally agrees:

- that the tenderer has been informed of the purpose of the collection and processing of its personal information as defined in the Protection of Personal Information Act of 2013 ("**POPIA**"), which, for the avoidance of doubt is for, and in relation to, the tender process and the negotiation, conclusion,

performance and enforcement of the ensuing agreement, if applicable, as well as for the City of Cape Town's reporting purposes;

- to the collection and processing of the tenderer's personal information by the City of Cape Town and agrees to make available to the City of Cape Town, all information reasonably required by the City of Cape Town for the above purposes;

- that the personal information the City of Cape Town collects from the tenderer or about the tenderer may be further processed for other activities and/or purposes which are lawful, reasonable, relevant and not excessive in relation to the purposes set out above, for which it was originally collected;

- that, the tenderer indemnifies the City of Cape Town and its officials, employees, and directors and undertakes to keep the City of Cape Town and its officials, employees, and directors indemnified in respect of any claim, loss, demands, liability, costs and expenses of whatsoever nature which may be made against the City of Cape Town (including the costs incurred in defending or contesting any such claim) in relation to the tenderer or the tenderer's employees', representatives' and/or sub-contractors' non-compliance with POPIA and/or the City of Cape Town's failure to obtain the tenderer's consent or to notify the tenderer of the reason for the processing of the tenderer's personal information;

- to the disclosure of the tenderer's personal information by the City of Cape Town to any third party, where the City of Cape Town has a legal or contractual obligation to disclose such personal information to the third party (or a legitimate interest exits therein);

- that, under POPIA, the tenderer may request to access, confirm, request the correction, destruction, or deletion of, or request a description of, personal information held by the City of Cape Town in relation to you, subject to applicable law; and

- that under POPIA, subject to applicable law, the tenderer also has the right to be notified of a personal information breach and the right to object to, or restrict, the City of Cape Town's processing of its personal information.

TENDERERS MUST NOTE THAT WHEREVER THIS DOCUMENT REFERS TO ANY PARTICULAR TRADE MARK, NAME, PATENT, DESIGN, TYPE, SPECIFIC ORIGIN OR PRODUCER, SUCH REFERENCE SHALL BE DEEMED TO BE ACCOMPANIED BY THE WORDS 'OR EQUIVALENT"

(2) CONDITIONS OF TENDER

1. General

2.1 Actions

2.1.1.1 The City of Cape Town (CCT) and each tenderer submitting a tender offer shall comply with these Conditions of Tender. In their dealings with each other, they shall discharge their duties and obligations as set out in these Conditions of Tender, timeously and with integrity, and behave equitably, honestly and transparently, comply with all legal obligations.

The parties agree that this tender, its evaluation and acceptance and any resulting contract shall also be subject to the Employer's Supply Chain Management Policy ('SCM Policy') that was applicable on the date the bid was advertised, save that if the Employer adopts a new SCM Policy which contemplates that any clause therein would apply to the contract emanating from this tender, such clause shall also be applicable to that contract. Please refer to this document contained on the Employer's website.

Abuse of the supply chain management system is not permitted and may result in the tender being rejected, cancellation of the contract, restriction of the supplier, and/or the exercise by the City of any other remedies available to it as described in the SCM Policy.

2.1.1.2 The CCT, the tenderer and their agents and employees involved in the tender process shall avoid conflicts of interest and where a conflict of interest is perceived or known, declare any such conflict of interest, indicating the nature of such conflict. Tenderers shall declare any potential conflict of interest in their tender submissions. Employees, agents and advisors of the CCT shall declare any conflict of interest to the CCT at the start of any deliberations relating to the procurement process or as soon as they become aware of such conflict, and abstain from any decisions where such conflict exists or recuse themselves from the procurement process, as appropriate.

2.1.1.3 The CCT shall not seek, and a tenderer shall not submit a tender, without having a firm intention and capacity to proceed with the contract.

2.1.2 Interpretation

2.1.2.1 The additional requirements contained in the returnable documents are part of these Conditions of Tender.

2.1.1.2 These Conditions of Tender and returnable schedules which are required for tender evaluation purposes, shall form part of the contract arising from the invitation to tender.

2.1.3 Communication during tender process
Verbal or any other form of communication, from the CCT, its employees, agents or advisors during site visits/clarification meetings or at any other time prior to the award of the Contract, will not be regarded as binding on the CCT, <u>unless communicated by the CCT in writing to suppliers by its Director: Supply Chain Management or his nominee</u>.

2.1.4 The CCT's right to accept or reject any tender offer or part there-off.

2.1.4.1 The CCT may accept or reject any tender offer and may cancel the tender process or reject all tender offers at any time before the formation of a contract. The CCT may, prior to the award of the tender, cancel a tender if:

(a) due to changed circumstances, there is no longer a need for the services, works or goods requested; or
(b) funds are no longer available to cover the total envisaged expenditure; or
(c) no acceptable tenders are received;
(d) there is a material irregularity in the tender process; or
(e) the parties are unable to negotiate market related pricing.

The CCT shall not accept or incur any liability to a tenderer for such cancellation or rejection, but will give written reasons for such action upon receiving a written request to do so.

2.1.5   Procurement procedures

2.1.5.1 General

Unless otherwise stated in the tender conditions, a contract will be concluded with the tenderer who scores the highest number of tender adjudication points.

Schedules A, B, C, D, E and F will be grouped and awarded collectively/ in its entirety, subject to the successful implementation of the pilot project; to a Main and Alternative bidder
The Alternative bidder will be appointed should the Main service provider not be able to successfully execute the implementation of the pilot project.

If insufficient responsive bids are received, the CCT reserves the right to appoint fewer tenderers, or not to appoint any tenderers at all.

The contract period shall be for a period of ten (10) years, but not exceeding 10 financial years from the commencement date of the contract. It is the intention of the City of Cape Town to award this tender subject to application of Section 33 of the Local Government Municipal Finance Management Act 56 of 2003, for ten (10) years, whereby this tender will be valid for a period longer than the regulatory condition of only three (3) financial years. The tender will be valid for the initial period of 3-years but not exceeding the 3rd financial year from contract commencement date. Thereafter, an additional 7-year term will apply subject to the City of Cape Town's Council approval and successful application of the MFMA Section 33 process during the award phase of the tender.

2.1.5.2 Proposal procedure using the two stage-system

A TWO-STAGE SYSTEM WILL BE FOLLOWED.

Only those tenderers who attended both the compulsory clarification meeting, and compulsory site visit as detailed in clause 2.2.1.1.3 of the Eligibility Criteria, will be considered for evaluation.

The tender will be evaluated in two stages according to the predetermined evaluation criteria as set out below

STAGE 1 – FUNCTIONAL EVALUATION

This stage will purely evaluated based on the functionality requirements.

Stage 1 will be based on the functional requirements/ capability of the tenderer to successfully execute the project.

1. No rates/ costing is applicable to this stage.

2. The tender offer will be evaluated in terms of clauses 2.2.1.1.3 (OSM Accreditation) and 2.2.1.1.4 (Functionality) of the Eligibility Criteria.

3. Only those offers who comply with clauses 2.2.1.1.3 and meet the minimum score for Functionality as detailed in clause 2.2.1.1.4 will be invited to continue to Stage 2.

STAGE 2 – PRODCUTS, PRICE AND PREFERENCE

1. Only those tenderers who have pre-qualified, or successfully met the evaluation criteria in Stage 1 will be afforded the opportunity to submit final technical and priced offers.

2. This evaluation will be in terms of your solution / products based on the tender requirements/ specifications.

3. Price Schedule to be completed in full.

4. The City reserves the right to request tenderers to come and present their presentations

5. The applicable price/ preference point system will be applied to those offers confirmed as responsive.

2.1.5.3 Nomination of Alternative Bidder
Alternative Bidder means a bidder, identified at the time of awarding a bid that will be considered for award should the contract be terminated for any reason whatsoever. In the event that a contract is terminated during the execution thereof, the CCT may consider the award of the contract, or non-award, to the alternative bidder in terms of the procedures included in its SCM Policy.

2.1.6 Objections, complaints, queries and disputes/ Appeals in terms of Section 62 of the Systems Act/ Access to court

2.1.6.1 Disputes, objections, complaints and queries
In terms of Regulations 49 and 50 of the Local Government: Municipal Finance Management Act, 56 of 2003 Municipal Supply Chain Management Regulations (Board Notice 868 of 2005):

Persons aggrieved by decisions or actions taken by the City of Cape Town in the implementation of its supply chain management system, may lodge within 14 days of the decision or action, a written objection or complaint or query or dispute against the decision or action.

2.1.6.2 Appeals

(a) In terms of Section 62 of the Local Government: Municipal Systems Act, 32 of 2000 a person whose rights are affected by a decision taken by the City, may appeal against that decision by giving written notice of the appeal and reasons to the City Manager within 21 days of the date of the notification of the decision.

(b) An appeal must contain the following:

1. Must be in writing
2. It must set out the reasons for the appeal
3. It must state in which way the Appellant's rights were affected by the decision;
4. It must state the remedy sought; and
5. It must be accompanied with a copy of the notification advising the person of the decision

(c) The relevant City appeal authority must consider the appeal and **may confirm, vary or revoke** the decision that has been appealed, but no such revocation of a decision may detract from any rights that may have accrued as a result of the decision.

2.1.6.3 Right to approach the courts and rights in terms of Promotion of Administrative Justice Act, 3 of 2000 and Promotion of Access to Information Act, 2 of 2000

The sub- clauses above do not influence any affected person's rights to approach the High Court at any time or its rights in terms of the Promotion of Administrative Justice Act (PAJA) and Promotion of Access to Information Act (PAIA).

2.1.6.4 All requests referring to sub clauses 2.1.6.1 and 2.1.6.2 must be submitted in writing to:

The City Manager - C/o the Manager: Legal Compliance Unit, Legal Services Department, Corporate Services Directorate

Via hand delivery at: 20th Floor, Tower Block, 12 Hertzog Boulevard, Cape Town 8001

Via post at: Private Bag X918, Cape Town, 8000

Via fax at: 021 400 5963 or 021 400 5830

Via email at: MSA. Appeals@capetown.gov.za

2.1.6.5 All requests referring to clause 2.1.6.3 ns must be submitted in writing to:

The City Manager - C/o the Manager: Access to Information Unit, Corporate Services Directorate

Via hand delivery at: 20th Floor, Tower Block, 12 Hertzog Boulevard, Cape Town 8001

Via post at: Private Bag X918, Cape Town, 8000

Via fax at: 086 202 9982

Via email at: Access2info.Act@capetown.gov.za

2.1.7   City of Cape Town Supplier Database Registration
Tenderers are required to be registered on the CCT Supplier Database as a service provider. Tenderers must register as such upon being requested to do so in writing and within the period contained in such a request, failing which no orders can be raised or payments processed from the resulting contract. In the case of Joint Venture partnerships this requirement will apply individually to each party of the Joint Venture.

Tenderers who wish to register on the City of Cape Town's Supplier Database may collect registration forms from the Supplier Management Unit located within the Supplier Management / Registration Office, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town (Tel 021 400 9242/3/4/5). Registration forms and related information are also available on the City of Cape Town's website www.capetown.gov.za (follow the Supply Chain Management link to Supplier registration).

It is each tenderer's responsibility to keep all the information on the CCT Supplier Database updated.

2.1.8   National Treasury Web Based Central Supplier Database (CSD) Registration
Tenderers are required to be registered on the National Treasury Web Based Central Supplier Database (CSD) as a service provider. Tenderers must register as such upon being requested to do so in writing and within the period contained in such a request, failing which no orders can be raised or payments processed from the resulting contract. In the case of Joint Venture partnerships this requirement will apply individually to each party of the Joint Venture.

Tenderers who wish to register on the National Treasury Web Based Central Supplier Database (CSD) may do so via the web address **https://secure.csd.gov.za**.

It is each tenderer's responsibility to keep all the information on the National Treasury Web Based Central Supplier Database (CSD) updated.

Protection of Personal Information
The parties agree that this tender, its evaluation and acceptance and any resulting contract shall also be subject to the Employer's Supply Chain Management Policy ('SCM Policy') and Privacy Notice that was applicable on the date the bid was advertised, save that if the Employer adopts a new SCM Policy and/or Privacy Notice which contemplates that any clause therein would apply to the contract emanating from this tender, such clause shall also be applicable to that contract. Please refer to these documents contained on the Employer's website. The latest version of the document can be found in URL below:

https://resource.capetown.gov.za/documentcentre/Documents/Bylaws%20and%20policies/Supply%20Chain%20Management%20Policy.pdf '

2.2 Tenderer's obligations

2.2.1 Eligibility Criteria

2.2.1.1 Tenderers are obligated to submit a tender offer that complies in all aspects to the conditions as detailed in this tender document. Only those tenders that comply in all aspects with the tender conditions, specifications, pricing instructions and contract conditions will be declared to be responsive.

2.2.1.1.1 Submit a tender offer
Only those tender submissions from which it can be established that a clear, irrevocable and unambiguous offer has been made to CCT, by whom the offer has been made and what the offer constitutes, will be declared responsive.

2.2.1.1.2 Compliance with requirements of CCT SCM Policy and procedures
Only those tenders that are compliant with the requirements below will be declared responsive:

(a) A completed **Details of Tenderer** to be provided (applicable schedule to be completed);
(b) A completed **Certificate of Authority for Partnerships/ Joint Ventures/ Consortiums** to be provided authorising the tender to be made and the signatory to sign the tender on the partnership /joint venture/consortium's (applicable schedule to be completed);
(c) A copy of the partnership / joint venture / consortium agreement to be provided.
(d) A completed **Declaration of Interest – State Employees** to be provided and which does not indicate any non-compliance with the legal requirements relating to state employees (applicable schedule to be completed);
(e) A completed **Declaration – Conflict of Interest and Declaration of Bidders' past Supply Chain Management Practices** to be provided and which does not indicate any conflict or past practises that renders the tender non-responsive based on the conditions contained thereon (applicable schedules to be completed);
(f) A completed **Certificate of Independent Bid Determination** to be provided and which does not indicate any non-compliance with the requirements of the schedule (applicable schedule to be completed);
(g) The tenderer (including any of its directors or members), has not been restricted in terms of abuse of the Supply Chain Management Policy,
(h) The tenderer's tax matters with SARS are in order, or the tenderer is a foreign supplier that is not required to be registered for tax compliance with SARS;
(i) The tenderer is not an advisor or consultant contracted with the CCT whose prior or current obligations creates any conflict of interest or unfair advantage,
(j) The tenderer is not a person, advisor, corporate entity or a director of such corporate entity, involved with the bid specification committee;
(k) A completed **Authorisation for the Deduction of Outstanding Amounts Owed to the City of Cape Town** to be provided and which does not indicate any details that renders the tender non-responsive based on the conditions contained thereon (applicable schedules to be completed);
(l) The tenderer (including any of its directors or members), has not been found guilty of contravening the Competition Act 89 of 1998, as amended from time to time;
(m) The tenderer (including any of its directors or members), has not been found guilty on any other basis listed in the Supply Chain Management Policy.

2.2.1.1.3 Compulsory clarification and site meeting

Tenderers are required to attend **BOTH** a compulsory clarification meeting as well as compulsory site meeting, of which details will be provided at the briefing session. Tenderers may familiarise themselves with aspects of the proposed work, services or supply and pose questions.

Details of the meeting(s) are stated in the General Tender Information.

Only those tenders submitted by tenderers whose attendance at **BOTH** these meeting have been recorded, will be declared responsive

2.2.1.1.4   Mandatory Requirement – OSM Authorisation/ Accreditation

Tenderers must be authorised or accredited by the Original Software Manufacturer (OSM) or copyright holder to sell, distribute, implement and support the software solution and manage any warranty processes and escalations as and when required. Alternatively, should the authorization / accreditation be from a distributor, then a proof of authorization authorizing the distributor to resell and/or authorize others by the OSM or copyright holder, must be submitted.

Tenderers are to submit, either with their tender submission (attached to Schedule 15A), or within a specified timeframe after being requested to do so; proof of authority from the OSM to sell/maintain/ support the products of the OSM or copyright holder.

2.2.1.1.5   Minimum score for functionality

Only those tenders submitted by tenderers who achieve the minimum score for functionality as stated below will be declared responsive. **In order for the Bid Evaluation Committee to score the offers submitted tenderers MUST complete Schedules 15B, 15C, 15D, 15E and 15F of the tender.**

The description of the functionality criteria and the maximum possible score for each is shown in the table below. The score achieved for functionality will be the sum of the scores achieved, in the evaluation process, for the individual criteria.

Tenderers will be evaluated according to the name of the entity (Company, Partnership, Consortium, etc.) as provided in Section 3, Details of Tenderer.

Item	Evaluation Criteria	Applicable values	Points	Weight
2.2.1.1.5.1	**Experience of the Tendering Entity in terms of providing RM&DM&CM Solutions** Tenderer to demonstrate knowledge and experience in **all** of the following areas i.e. supply, implementation, migration, maintaining and supporting Records Management & Case Management and Document Management(RCM&DM) Solutions. Please provide verifiable evidence of the number of continuous years the tenderer has been actively providing RM&DM&CM&CM Solutions to their client base. This evidence may be in the form of reference letters, on the referee's letterhead, specifying the details and scope of the RM&DM&CM solution, the number of continuous years they have been actively receiving the RM&DM&CM solution from the tenderer, as well as all the referee's verifiable contact details. Scoring will be based on the continuous years providing RM&DM&CM Solutions, as confirmed in the evidence in all three areas. Please respond to this functional requirement and provide evidence to your response in **Schedule 15B: Information to Be Provided with The Tender.**	• 0 years • > 0 and < 5 years • ≥ 5 and < 10 years • ≥10 years	0 points 10 points 15 points 20 points	20 Points

Item	Evaluation Criteria	Applicable values	Points	Weight
2.2.1.1.5.2	**Size of organisation where a RM&DM&CM Solution has been implemented by the tendering entity** Tenderer to demonstrate the size of the organisation (users) where a RM&DM&CM solution has been implemented at their clients indicating the number of users. Please provide verifiable evidence in the form of references, specifying the number of users, as well as all the referee's contact details. Scoring will be based on the total number of the users, as provided in the evidence. Please respond to this functional requirement and provide evidence to your response in **Schedule 15C: Information to Be Provided with The Tender.**	• < 500 users • ≥ 500 but < 10 000 User • ≥ 10 000 but < 20 000 Users • ≥ 20 000 and < 30 000 users • ≥ 30 000 users	0 points 4 points 10 points 16 points 20 points	20 Points
2.2.1.1.5.3	**Operational Experience Requirement of the tendering entity** Tenderer to demonstrate experience in post implementation software maintenance and support of a RM&DM&CM Solution for their clients. Refer to **Section 13.7** in specifications for the overview of the Support and Maintenance requirements Please provide verifiable evidence in the form of references, specifying the number of years providing operational maintenance and support, as well as all the referee's contact details. Scoring will be based on the total number of years, as confirmed in the provided evidence. Please respond to this functional requirement and provide evidence to your response in **Schedule 15D: Information to Be Provided with The Tender.**	• 0 years • > 0 and < 5 years • ≥ 5 and < 10 years • ≥ 10 years	0 points 10 points 15 points 20 points	20 Points

Item	Evaluation Criteria	Applicable values	Points	Weight
2.2.1.1.5.4	**Comparable Project / Size of the Client** Tenderer to demonstrate where RM&DM&CM solutions have been implemented within the last 5 years, with scope and clients comparable to the scope and requirements of the City of Cape Town as indicated in the specifications of this tender document. Refer **Section 13.3** in specifications for the overview of the City's environment. Please provide verifiable evidence, identifying the client indicating the size of the organisation in RM&DM&CM of number of system users, where a RM&DM&CM solution was successfully implemented within the last 5 years. This evidence may be in the form of reference letters, on the referee's letterhead with the referee's verifiable contact details to be included. Clearly identify if the client is a Public Sector client. Scoring will be based on the number of clients, as confirmed in the evidence. For the purposes of scoring, an acceptable Comparable Project/ Client must have had a minimum of 20 000 system users. A Project / Client with less than 20 000 system users will therefore not be scored. This excludes clients within the Public Sector. Please respond to this functionality requirement and provide evidence to your response in **Schedule 15E: Information to be Provided with The Tender**.	• 0 clients • < 3 clients • ≥ 3 but < 5 clients • ≥ 3 but < 5 clients with at least 1 client in the Public sector • ≥ 5 clients • ≥ 5 clients with at least 1 client in the Public sector	0 points 4 points 8 points 12 points 16 points 20 points	20 Points

Item	Evaluation Criteria	Applicable values	Points	Weight
2.2.1.1.5.5	**Previous Implementation Project Value** Tenderer to demonstrate credibility with projects similar to the scope as required by the City in implementing, maintaining and supporting a RM&DM&CM Solution within the last 5 years. Refer to Section 13.1 in the specifications for the overview of the City's environment. The tenderer must submit a list of successfully completed project(s) **within the last 5 years,** showing the value of the project, name of the client and verifiable contact details. Scoring will be based on the cumulative value of the completed and projects in progress within the last 5 years. Please respond to this functionality requirement and provide evidence to your response in **Schedule 15F: Information to Be Provided with The Tender.**	• R0 • < R25M • ≥ R25M and < R50M • ≥ R50M and < R75M • ≥ R75M and ≤ R100M • > R100M	0 points 4 points 8 points 12 points 16 points 20 points	20 Points
	Total			**100 Points**

The minimum qualifying score for functionality is **70** out of a maximum of **100 achievable points.**

Where the entity tendering is a Joint Venture the tender must be accompanied by a statement describing exactly what aspects of the work will be undertaken by each party to the joint venture.

Tenderers shall ensure that all relevant information has been submitted with the tender offer in the prescribed format to ensure optimal scoring of functionality points for each Evaluation Criteria. Failure to provide all information IN THIS TENDER SUBMISSION could result in the tenderer not being able to achieve the specified minimum scoring.

2.2.1.1.6 Technical Schedule

In order for the Bid Evaluation Committee to determine whether the OSM Solutions offered are functional, and to the required specification of the City of Cape Town, tenderers MUST complete the applicable Technical Schedules either with their tender submission after being requested to do so:
a) Schedule 15G: RM&DM&CM Solution

2.2.1.1.7 Local production and content
Not applicable to the tender.

2.2.1.1.8 Pre-qualification criteria for preferential procurement
Not applicable to the tender.

2.2.1.1.9 Provision of samples
Not Applicable to the tender

2.2.2 Cost of tendering
The CCT will not be liable for any costs incurred in the preparation and submission of a tender offer, Including the costs of any testing necessary to demonstrate that aspects of the offer complies with requirements.

2.2.3 Check documents
The documents issued by the CCT for the purpose of a tender offer are listed in the index of this tender

document.

Before submission of any tender, the tenderer should check the number of pages, and if any are found to be missing or duplicated, or the figures or writing is indistinct, or if the Price Schedule contains any obvious errors, the tenderer must apply to the CCT at once to have the same rectified.

2.2.4   Confidentiality and copyright of documents
Treat as confidential all matters arising in connection with the tender. Use and copy the documents issued by the CCT only for the purpose of preparing and submitting a tender offer in response to the invitation.

2.2.5   Reference documents
Obtain, as necessary for submitting a tender offer, copies of the latest versions of standards, specifications, Conditions of Contract and other publications, which are not attached but which are incorporated into the tender documents by reference.

2.2.6   Acknowledge and comply with notices
Acknowledge receipt of notices to the tender documents, which the CCT may issue, fully comply with all instructions issued in the notices, and if necessary, apply for an extension of the closing time stated on the front page of the tender document, in order to take the notices into account. Notwithstanding any requests for confirmation of receipt of notices issued, the tenderer shall be deemed to have received such notices if the CCT can show proof of transmission thereof via electronic mail, facsimile or registered post.

2.2.7   Clarification meeting
Attend, where required, a clarification meeting at which tenderers may familiarise themselves with aspects of the proposed work, services or supply and pose questions. Details of the meeting(s) are stated in the General Tender Information.

Tenderers should be represented at the site visit/clarification meeting by a person who is suitably qualified and experienced to comprehend the implications of the work involved.

2.2.8   Seek clarification
Request clarification of the tender documents, if necessary, by notifying the CCT at least one week before the closing time stated in the General Tender Information, where possible.

2.2.9   Pricing the tender offer

2.2.9.1 Comply with all pricing instructions as stated on the Price Schedule.

2.2.10   Alterations to documents
Do not make any alterations or additions to the tender documents, except to comply with instructions issued by the CCT in writing, or necessary to correct errors made by the tenderer. All signatories to the tender offer shall initial all such alterations.

2.2.11   Alternative tender offers

2.2.11.1   Unless otherwise stated in the tender conditions submit alternative tender offers only if a main tender offer, strictly in accordance with all the requirements of the tender documents, is also submitted.

If a tenderer wishes to submit an alternative tender offer, he shall do so as a separate offer on a complete set of tender documents. The alternative tender offer shall be submitted in a separate sealed envelope clearly marked "Alternative Tender" in order to distinguish it from the main tender offer.

Only the alternative of the highest ranked acceptable main tender offer (that is, submitted by the same tenderer) will be considered, and if appropriate, recommended for award.

Alternative tender offers of any but the highest ranked main tender offer will not be considered.

An alternative of the highest ranked acceptable main tender offer that is priced higher than the main tender offer may be recommended for award, provided that the ranking of the alternative tender offer is higher than the ranking of the next ranked acceptable main tender offer.

The CCT will not be bound to consider alternative tenders and shall have sole discretion in this regard.

In the event that the alternative is accepted, the tenderer warrants that the alternative offer complies in all respects with the CCT's standards and requirements.

2.2.11.2 Accept that an alternative tender offer may be based only on the criteria stated in the tender conditions or criteria otherwise acceptable to the CCT.

2.2.12 **Submitting a tender offer**

2.2.12.1 Submit one tender offer only on the original tender documents as issued by the CCT, either as a single tendering entity or as a member in a joint venture to provide the whole of the works, services or supply identified in the contract conditions and described in the specifications. Only those tenders submitted on the tender documents as issued by the CCT together with all Returnable Schedules duly completed and signed will be declared responsive.

2.2.12.2 Return the entire document to the CCT after completing it in its entirety, either electronically (if they were issued in electronic format) or by writing legibly in non-erasable ink.

2.2.12.3 Submit the parts of the tender offer communicated on paper as an original with an English translation for any part of the tender submission not made in English.

1 (One) copy(ies) of the following elements of the bid submission must be submitted separately bound in the same envelope where possible:

Part	Heading
5	Pricing Schedules
6	Supporting Schedules
All other attachments submitted by bidder – **Please clearly reference all attachments**	

2.2.12.4 Sign the original tender offer where required in terms of the tender conditions. The tender shall be signed by a person duly authorised to do so. Tenders submitted by joint ventures of two or more firms shall be accompanied by the document of formation of the joint venture or any other document signed by all parties, in which is defined precisely the conditions under which the joint venture will function, its period of duration, the persons authorised to represent and obligate it, the participation of the several firms forming the joint venture, and any other information necessary to permit a full appraisal of its functioning. Signatories for tenderers proposing to contract as joint ventures shall state which of the signatories the lead partner is.

2.2.12.5 Where a two-envelope system is required in terms of the tender conditions, place and seal the returnable documents listed in the tender conditions in an envelope marked "financial proposal" and place the remaining returnable documents in an envelope marked "technical proposal". Each envelope shall state on the outside the CCT's address and identification details stated in the General Tender Information, as well as the tenderer's name and contact address.

2.2.12.6 Seal the original tender offer and copy packages together in an outer package that states on the outside only the CCT's address and identification details as stated in the General Tender Information. If it is not possible to submit the original tender and the required copies (see 2.2.12.3) in a single envelope, then the tenderer must seal the original and each copy of the tender offer as separate packages marking the packages as "ORIGINAL" and "COPY" in addition to the aforementioned tender submission details.

2.2.12.7 Accept that the CCT shall not assume any responsibility for the misplacement or premature opening of the tender offer if the outer package is not sealed and marked as stated.

2.2.12.8 Accept that tender offers submitted by facsimile or e-mail will be rejected by the CCT, unless stated otherwise in the tender conditions.

2.2.12.9 By signing the offer part of the Form of Offer in section **(4) Form of Offer and Acceptance** the tenderer warrants that all information provided in the tender submission is true and correct.

2.2.12.10 Tenders must be properly received and deposited in the designated tender box (as detailed on the front page of this tender document) on or before the closing date and before the closing time, in the

relevant tender box at the Tender & Quotation Boxes Office situated on the 2nd floor, Concourse Level, Civic Centre, 12 Hertzog Boulevard, Cape Town. If the tender submission is too large to fit in the allocated box, please enquire at the public counter for assistance.

2.2.12.11   The tenderer must record and reference all information submitted contained in other documents for example cover letters, brochures, catalogues, etc. in the returnable schedule titled **List of Other Documents Attached by Tenderer**.

2.2.13   **Information and data to be completed in all respects**

Accept that tender offers, which do not provide all the data or information requested completely and in the form required, may be regarded by the CCT as non-responsive.

2.2.14   **Closing time**

2.2.14.1   Ensure that the CCT receives the tender offer at the address specified in the General Tender Information prior to the closing time stated on the front page of the tender document.

2.2.14.2   Accept that, if the CCT extends the closing time stated on the front page of the tender document for any reason, the requirements of these Conditions of Tender apply equally to the extended deadline.

2.2.14.3   Accept that, the CCT shall not consider tenders that are received after the closing date and time for such a tender (late tenders).

2.2.15   **Tender offer validity and withdrawal of tenders**

2.2.15.1   Warrants that the tender offer(s) remains valid, irrevocable and open for acceptance by the CCT at any time for a period of 120 days after the closing date stated on the front page of the tender document.

2.2.15.   Notwithstanding the period stated above, bids shall remain valid for acceptance for a period of twelve (12) months after the expiry of the original validity period, unless the City is notified in writing of anything to the contrary by the bidder. The validity of bids may be further extended by a period of not more than six months subject to mutual agreement and administrative processes and upon approval by the City Manager.

2.2.15.3   A tenderer may request in writing, after the closing date, that the tender offer be withdrawn. Such withdrawal will be permitted or refused at the sole discretion of the CCT after consideration of the reasons for the withdrawal, which shall be fully set out by the tenderer in such written request for withdrawal. Should the tender offer be withdrawn in contravention hereof, the tenderer agrees that:

a)   it shall be liable to the CCT for any additional expense incurred or losses suffered by the CCT in having either to accept another tender or, if new tenders have to be invited, the additional expenses incurred or losses suffered by the invitation of new tenders and the subsequent acceptance of any other tender;

b)   the CCT shall also have the right to recover such additional expenses or losses by set-off against monies which may be due or become due to the tenderer under this or any other tender or contract or against any guarantee or deposit that may have been furnished by the tenderer or on its behalf for the due fulfilment of this or any other tender or contract. Pending the ascertainment of the amount of such additional expenses or losses, the CCT shall be entitled to retain such monies, guarantee or deposit as security for any such expenses or loss.

2.2.16   **Clarification of tender offer, or additional information, after submission**
Provide clarification of a tender offer, or additional information, in response to a written request to do so from the CCT during the evaluation of tender offers within the time period stated in such request. No change in the competitive position of tenderers or substance of the tender offer is sought, offered, or permitted.

Note: This clause does not preclude the negotiation of the final terms of the contract with a preferred tenderer following a competitive selection process, should the CCT elect to do so.

Failure, or refusal, to provide such clarification or additional information within the time for submission stated in the CCT's written request may render the tender non-responsive.

2.2.17 Provide other material

2.2.17.1 Provide, on request by the CCT, any other material that has a bearing on the tender offer, the tenderer's commercial position (including joint venture agreements), preferencing arrangements, or samples of materials, considered necessary by the CCT for the purpose of the evaluation of the tender. Should the tenderer not provide the material, or a satisfactory reason as to why it cannot be provided, by the time for submission stated in the CCT's request, the CCT may regard the tender offer as non-responsive.

2.2.17.2 Provide, on written request by the CCT, where the transaction value inclusive of VAT **exceeds R 10 million**:

    a)   audited annual financial statement for the past 3 years, or for the period since establishment if established during the past 3 years, if required by law to prepare annual financial statements for auditing;

    b)   a certificate signed by the tenderer certifying that the tenderer has no undisputed commitments for municipal services towards a municipality or other service provider in respect of which payment is overdue for more than 30 days;

    c)   particulars of any contracts awarded to the tenderer by an organ of state during the past five years, including particulars of any material non-compliance or dispute concerning the execution of such contract;

    d)   a statement indicating whether any portion of the goods or services are expected to be sourced from outside the Republic, and, if so, what portion and whether any portion of payment from the municipality or municipal entity is expected to be transferred out of the Republic.

Each party to a Consortium/Joint Venture shall submit separate certificates/statements in the above regard.

2.2.17.3 Tenderers undertake to fully cooperate with the CCT's external service provider appointed to perform a due diligence review and risk assessment upon receipt of such written instruction from the CCT.

2.2.18 Samples, Inspections, tests and analysis
Provide access during working hours to premises for inspections, tests and analysis as provided for in the tender conditions or specifications.

If the **Specification** requires the tenderer to provide samples, these shall be provided strictly in accordance with the instructions set out in the Specification.

If such samples are not submitted as required in the bid documents or within any further time stipulated by the CCT in writing, then the bid concerned may be declared non-responsive.

The samples provided by all successful bidders will be retained by the CCT for the duration of any subsequent contract. Bidders are to note that samples are requested for testing purposes therefore samples submitted to the CCT may not in all instances be returned in the same state of supply and in other instances may not be returned at all. Unsuccessful bidders will be advised by the Project Manager or dedicated CCT Official to collect their samples, save in the aforementioned instances where the samples would not be returned.

2.2.19 Certificates
The tenderer must provide the CCT with all certificates as stated below:

2.2.19.1 Broad-Based Black Economic Empowerment Status Level Documentation
In order to qualify for preference points, it is the responsibility of the tenderer to submit documentary proof, either as certificates, sworn affidavits or any other requirement prescribed in terms of the B-BBEE Act, of its B-BBEE status level of contribution in accordance with the applicable Codes of good practise as issued by the Department of Trade and Industry, to the CCT at the Supplier Management Unit located within the Supplier Management / Registration Office, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town (Tel 021 400 9242/3/4/5) or included with the tender submission.

Consortiums/Joint Ventures will qualify for preference points, provided that the **entity** submits the relevant certificate/scorecard in accordance with the applicable codes of good practise. Note that,

in the case of unincorporated entities, a verified consolidated B-BBEE scorecard must be submitted in the form of a certificate with the tender.

Tenderers are further referred to the content of the **Preference Schedule** for the full terms and conditions applicable to the awarding of preference points.

The applicable code for this tender is the **Information and Communication Technology (ICT) Charter** unless in possession of a valid sector certificate.

The tenderer shall indicate in Section 4 of the **Preference Schedule** the Level of Contribution in respect of the enterprise status or structure of the tendering entity (the supplier).

2.2.19.2   Evidence of tax compliance
Tenderers shall be registered with the South African Revenue Service (SARS) and their tax affairs must be in order and they must be tax compliant subject to the requirements of clause 2.2.1.1.2.h. In this regard, it is the responsibility of the Tenderer to submit evidence in the form of a valid Tax Clearance Certificate issued by SARS to the CCT at the Supplier Management Unit located within the Supplier Management / Registration Office, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town (Tel 021 400 9242/3/4/5), or included with this tender. The tenderer must also provide its Tax Compliance Status PIN number on the **Details of Tenderer** pages of the tender submission.

Each party to a Consortium/Joint Venture shall submit a separate Tax Clearance Certificate.

Before making an award, the City must verify the bidder's tax compliance status. Where the recommended bidder is not tax compliant, the bidder should be notified of the non-compliant status and be requested to submit to the City, within 7 working days, written proof from SARS

that they have made arrangement to meet their outstanding tax obligations. The proof of tax compliance submitted by the bidder must be verified by the City via CSD or e-Filing. The City should reject a bid submitted by the bidder if such bidder fails to provide proof of tax compliance within the timeframe stated herein.

Only foreign suppliers who have answered "NO" to all the questions contained in the Questionnaire to Bidding Foreign Suppliers section on the **Details of Tenderer** pages of the tender submission, are not required to register for a tax compliance status with SARS.

2.2.20   Compliance with Occupational Health and Safety Act, 85 of 1993
Tenderers are to note the requirements of the Occupational Health and Safety Act, 85 of 1993. The Tenderer shall be deemed to have read and fully understood the requirements of the above Act and Regulations and to have allowed for all costs in compliance therewith.

In this regard the Tenderer shall submit **upon written request to do so by the CCT**, a Health and Safety Plan in sufficient detail to demonstrate the necessary competencies and resources to deliver the goods or services all in accordance with the Act, Regulations and Health and Safety Specification.

2.2.21   Claims arising from submission of tender

The tenderer warrants that it has:

a) inspected the Specifications and read and fully understood the Conditions of Contract.
b) read and fully understood the whole text of the Specifications and Price Schedule and thoroughly acquainted himself with the nature of the goods or services proposed and generally of all matters which may influence the Contract.
c) visited the site(s) where delivery of the proposed goods will take place, carefully examined existing conditions, the means of access to the site(s), the conditions under which the delivery is to be made, and acquainted himself with any limitations or restrictions that may be imposed by the Municipal or other Authorities in regard to access and transport of materials, plant and equipment to and from the site(s) and made the necessary provisions for any additional costs involved thereby.
d) requested the CCT to clarify the actual requirements of anything in the Specifications and Price Schedule, the exact meaning or interpretation of which is not clearly intelligible to the

Tenderer.
e) received any notices to the tender documents which have been issued in accordance with the CCT's Supply Chain Management Policy.

The CCT will therefore not be liable for the payment of any extra costs or claims arising from the submission of the tender.

2.3 The CCT's undertakings

2.3.1 Respond to requests from the tenderer

2.3.1.1 Unless otherwise stated in the Tender Conditions, respond to a request for clarification received up to one week (where possible) before the tender closing time stated on the front page of the tender document.

2.3.1.2 The CCT's representative for the purpose of this tender is stated on the General Tender Information page.

2.3.2 Issue Notices
If necessary, issue addenda in writing that may amend or amplify the tender documents to each tenderer during the period from the date the tender documents are available until one week before the tender closing time stated in the Tender Data. The Employer reserves its rights to issue addenda less than one week before the tender closing time in exceptional circumstances If, as a result a tenderer applies for an extension to the closing time stated on the front page of the tender document, the CCT may grant such extension and, shall then notify all tenderers who drew documents.

Notwithstanding any requests for confirmation of receipt of notices issued, the tenderer shall be deemed to have received such notices if the CCT can show proof of transmission thereof via electronic mail, facsimile or registered post.

2.3.3 Opening of tender submissions

2.3.3.1 Unless the two-envelope system is to be followed, open tender submissions in the presence of tenderers' agents who choose to attend at the time and place stated in the tender conditions.

Tenders will be opened immediately after the closing time for receipt of tenders as stated on the front page of the tender document, or as stated in any Notice extending the closing date and at the closing venue as stated in the General Tender Information.

2.3.3.2 Announce at the meeting held immediately after the opening of tender submissions, at the closing venue as stated in the General Tender Information, the name of each tenderer whose tender offer is opened and, where possible, the prices and the preferences indicated.

2.3.3.3 Make available a record of the details announced at the tender opening meeting on the CCT's website (http://www.capetown.gov.za/en/SupplyChainManagement/Pages/default.aspx.)

2.3.4 Two-envelope system

2.3.4.1 Where stated in the tender conditions that a two-envelope system is to be followed, open only the technical proposal of tenders in the presence of tenderers' agents who choose to attend at the time and place stated in the tender conditions and announce the name of each tenderer whose technical proposal is opened.

2.3.4. Evaluate the quality of the technical proposals offered by tenderers, then advise tenderers who have submitted responsive technical proposals of the time and place when the financial proposals will be opened. Open only the financial proposals of tenderers, who have submitted responsive technical proposals in accordance with the requirements as stated in the tender conditions, and announce the total price and any preferences claimed. Return unopened financial proposals to tenderers whose technical proposals were non responsive.

2.3.5 Non-disclosure
Not disclose to tenderers, or to any other person not officially concerned with such processes, information relating to the evaluation and comparison of tender offers and recommendations for the award of a contract, until after the award of the contract to the successful tenderer.

2.3.6   Grounds for rejection and disqualification
Determine whether there has been any effort by a tenderer to influence the processing of tender offers and instantly disqualify a tenderer (and his tender offer) if it is established that he engaged in corrupt or fraudulent practices.

2.3.7   Test for responsiveness

2.3.7.1 Appoint a Bid Evaluation Committee and determine after opening whether each tender offer properly received:
(a)   complies with the requirements of these Conditions of Tender,
(b)   has been properly and fully completed and signed, and
(c)   is responsive to the other requirements of the tender documents

2.3.7.2 A responsive tender is one that conforms to all the terms, conditions, and specifications of the tender documents without material deviation or qualification. A material deviation or qualification is one which, in the CCT's opinion, would:

(a) detrimentally affect the scope, quality, or performance of the goods, services or supply identified in the Specifications,
(b) significantly change the CCT's or the tenderer's risks and responsibilities under the contract, or
(c) affect the competitive position of other tenderers presenting responsive tenders, if it were to be rectified.

Reject a non-responsive tender offer, and not allow it to be subsequently made responsive by correction or withdrawal of any material deviation or qualification.

The CCT reserves the right to accept a tender offer which does not, in the CCT's opinion, materially and/or substantially deviate from the terms conditions, and specifications of the tender documents.

2.3.8   Arithmetical errors, omissions and discrepancies

2.3.8.1 Check the responsive tenders for:

(a) the gross misplacement of the decimal point in any unit rate;
(b) omissions made in completing the Price Schedule; or
(c) arithmetic errors in:
(d) line item totals resulting from the product of a unit rate and a quantity in the Price Schedule; or
(e) the summation of the prices; or
(f) calculation of individual rates.

2.3.8.2 The CCT must correct the arithmetical errors in the following manner:

(a)   Where there is a discrepancy between the amounts in words and amounts in figures, the amount in words shall govern.
(b)   If pricing schedules apply and there is an error in the line item total resulting from the product of the unit rate and the quantity, the line item total shall govern and the rate shall be corrected. Where there is an obviously gross misplacement of the decimal point in the unit rate, the line item total as tendered shall govern, and the unit rate shall be corrected.
(c)   Where there is an error in the total of the prices either as a result of other corrections required by this checking process or in the tenderer's addition of prices, the total of the prices shall govern and the tenderer will be asked to revise selected item prices (and their rates if Price Schedules apply) to achieve the tendered total of the prices.

Consider the rejection of a tender offer if the tenderer does not correct or accept the correction of the arithmetical error in the manner described above.

2.3.8.3 In the event of tendered rates or lump sums being declared by the CCT to be unacceptable to it because they are not priced, either excessively low or high, or not in proper balance with other rates or lump sums, the tenderer may be required to produce evidence and advance arguments in support of the tendered rates or lump sums objected to. If, after submission of such evidence and any further evidence requested, the CCT is still not satisfied with the tendered rates or lump sums objected to, it may request the tenderer to amend these rates and lump sums along the lines indicated by it.

The tenderer will then have the option to alter and/or amend the rates and lump sums objected to and such other related amounts as are agreed on by the CCT, but this shall be done without altering the tender offer in accordance with this clause.

Should the tenderer fail to amend his tender in a manner acceptable to and within the time stated by the CCT, the CCT may declare the tender as non-responsive.

2.3.9 **Clarification of a tender offer**
The CCT may, after the closing date, request additional information or clarification from tenderers, in writing on any matter affecting the evaluation of the tender offer or that could give rise to ambiguity in a contract arising from the tender offer, which written request and related response shall not change or affect their competitive position or the substance of their offer. Such request may only be made in writing by the Director: Supply Chain Management using any means as appropriate.

2.3.10 **Evaluation of tender offers**

2.3.10.1 **General**

2.3.10.1.1 Reduce each responsive tender offer to a comparative price and evaluate them using the tender evaluation methods and associated evaluation criteria and weightings that are specified in the tender conditions.

2.3.10.1.2 For evaluation purposes only, the effects of the relevant contract price adjustment methods will be considered in the determination of comparative prices as follows:

(a) If the selected method is based on bidders supplying rates or percentages for outer years, comparative prices would be determined over the entire contract period based on such rates or percentages.
(b) If the selected method is based on a formula, indices, coefficients, etc. that is the same for all bidders during the contract period, comparative prices would be the prices as tendered for year one.
(c) If the selected method is based on a formula, indices, coefficients, etc. that varies between bidders, comparative prices would be determined over the entire contract period based on published indices relevant during the 12 months prior to the closing date of tenders.
(d) If the selected method includes an imported content requiring rate of exchange variation, comparative prices would be determined based on the exchange rates tendered for the prices as tendered for year one. The rand equivalent of the applicable currency 14 days prior to the closing date of tender will be used (the CCT will check all quoted rates against those supplied by its own bank).
(e) If the selected method is based on suppliers' price lists, comparative prices would be the prices as tendered for year one.
(f) If the selected method is based on suppliers' price lists and / or rate of exchange, comparative prices would be determined as tendered for year one whilst taking into account the tendered percentage subject to rate of exchange (see sub clause (d) for details on the calculation of the rate of exchange).

2.3.10.1.3 Where the scoring of functionality forms part of a bid process, each member of the Bid Evaluation Committee must individually score functionality. The individual scores must then be interrogated and calibrated if required where there are significant discrepancies. The individual scores must then be added together and averaged to determine the final score.

2.3.10.2 **Decimal places**

Score financial offers, preferences and functionality, as relevant, to two decimal places.

2.3.10.3 **Scoring of tenders (price and preference)**

2.3.10.3.1 Points for price will be allocated in accordance with the formula set out in this clause based on the price per item / rates as set out in the **Price Schedule (Part 5)** based on the estimated quantities across the lifespan of the contract.

2.3.10.3.2 Points for preference will be allocated in accordance with the provisions of **Preference Schedule** and the table in this clause.

2.3.10.3.3 The terms and conditions of **Preference Schedule** as it relates to preference shall apply in all respects to the tender evaluation process and any subsequent contract.

2.3.10.3.4 Applicable formula:
The 90/10 price/preference points system will be applied to the evaluation of responsive tenders over a Rand value of R50'000'000 (all applicable taxes included), whereby the order(s) will be placed with the tenderer(s) scoring the highest total number of adjudication points.

Price shall be scored as follows:

$$Ps = 90 \times \left(1 - \frac{(Pt - Pmin)}{Pmin}\right)$$

Where: Ps is the number of points scored for price;
Pt is the price of the tender under consideration;
Pmin is the price of the lowest responsive tender.

Preference points shall be scored as follows:

Points will be awarded to tenderers who are eligible for preferences in respect of the B-BBEE level of contributor attained in terms of **Preference Schedule**.

A maximum of 10 tender adjudication points will be awarded for preference to tenderers with responsive tenders who are eligible for such preference, in accordance with the criteria listed below.

Up to **10** adjudication points (N_P) will be awarded for the level of B-BBEE contribution, in accordance with the tables below:

B-BBEE Status Level of Contributor	Number of Points for Preference
1	10
2	9
3	6
4	5
5	4
6	3
7	2
8	1
Non-compliant contributor	0

A non-compliant contributor is one who does not meet the minimum score for a level 8 contributor.

or, in respect of Exempted Micro Enterprises (EMEs):

Black Female Ownership of EME	Deemed B-BBEE Status Level of Contributor	Number of Points for Preference
less than 51%	4	5
at least 51% but less than 100%	2	9
100%	1	10

or, in respect of Qualifying Small Enterprises (QSEs):

Black Female Ownership of QSE	Deemed B-BBEE Status Level of Contributor	Number of Points for Preference
at least 51% but less than 100%	2	9
100%	1	10

The total number of adjudication points (N_T) shall be calculated as follows:

$N_T = Ps + N_P$

Where: Ps is the number of points scored for price;
         Np is the number of points scored for preference.

The Terms and conditions of the **Preference Schedule** shall apply in all respects to the tender evaluation process and any subsequent contract. **The total number of adjudication points (N_T) shall be calculated as follows:**

$N_T = Ps + N_P$

Where: Ps is the number of points scored for price;
         Np is the number of points scored for preference.

2.3.10.5   Risk Analysis
Notwithstanding compliance with regard to any requirements of the tender, the CCT will perform a risk analysis in respect of the following:

(a) reasonableness of the financial offer
(b) reasonableness of unit rates and prices
(c) the tenderer's ability to fulfil its obligations in terms of the tender document, that is, that the tenderer can demonstrate that he/she possesses the necessary professional and technical qualifications, professional and technical competence, financial resources, equipment and other physical facilities, managerial capability, reliability, capacity, experience, reputation, personnel to perform the contract, etc.; the CCT reserves the right to consider a tenderer's existing contracts with the CCT in this regard
(d) any other matter relating to the submitted bid, the tendering entity, matters of compliance, verification of submitted information and documents, etc.

The conclusions drawn from this risk analysis will be used by the CCT in determining the acceptability of the tender offer.

No tenderer will be recommended for an award unless the tenderer has demonstrated to the satisfaction of the CCT that he/she has the resources and skills required.

2.3.11   Negotiations with preferred tenderers
The CCT may negotiate the final terms of a contract with tenderers identified through a competitive tendering process as preferred tenderers provided that such negotiation:

(a)   does not allow any preferred tenderer a second or unfair opportunity;
(b)   is not to the detriment of any other tenderer; and
(c)   does not lead to a higher price than the tender as submitted.

If negotiations fail to result in acceptable contract terms the City Manager (or his delegated authority) may terminate the negotiations and cancel the tender, or invite the next ranked tenderer for negotiations. The original preferred tenderer should be informed of the reasons for termination of the negotiations. If the decision is to invite the next highest ranked tenderer for negotiations, the failed earlier negotiations may not be reopened by the CCT.

Minutes of any such negotiations shall be kept for record purposes.

The provisions of this clause will be equally applicable to any invitation to negotiate with any other tenderers.

In terms of the PPPFA Regulations, 2017, tenders must be cancelled in the event that negotiations fail to achieve a market related price with any of the three highest scoring tenderers.

2.3.12   Acceptance of tender offer
Notwithstanding any other provisions contained in the tender document, the CCT reserves the right to:

2.3.12.1   Accept a tender offer(s) which does not, in the CCT's opinion, materially and/or substantially deviate from the terms conditions, and specifications of the tender document.

2.3.12.2   Accept the whole tender or part of a tender or any item or part of any item or items from multiple manufacturers, or to accept more than one tender (in the event of a number of items being offered), and the CCT is not obliged to accept the lowest or any tender.

2.3.12.3   Accept the tender offer(s), if in the opinion of the CCT, it does not present any material risk and only if the tenderer(s):

(a)   is not under restrictions, has any principals who are under restrictions, or is not currently a supplier to whom notice has been served for abuse of the supply chain management system, preventing participation in the employer's procurement,

(b)   can, as necessary and in relation to the proposed contract, demonstrate that he or she possesses the professional and technical qualifications, professional and technical competence, financial resources, equipment and other physical facilities, managerial capability, reliability, experience and reputation, expertise and the personnel, to perform the contract,

(c)   has the legal capacity to enter into the contract,

(d)   is not insolvent, in receivership, under Business Rescue as provided for in chapter 6 of the Companies Act, 2008, bankrupt or being wound up, has his affairs administered by a court or a judicial officer, has suspended his business activities, or is subject to legal proceedings in respect of any of the foregoing, complies with the legal requirements, if any, stated in the tender data, and

(e)   is able, in the opinion of the employer, to perform the contract free of conflicts of interest.

If an award cannot be made in terms of anything contained herein, the Employer reserves the right to consider the next ranked tenderer(s).

2.3.12.4   Not to make an award, or revoke an award already made, where the implementation of the contract may result in reputational risk or harm to the City as a result of (inter alia):

(a) reports of poor governance and/or unethical behaviour;
(b) association with known family of notorious individuals;
(c) poor performance issues, known to the City;
(d) negative social media reports; and
(e) adverse assurance (e.g. due diligence) report outcomes.

2.3.12.5   The CCT reserves the right to nominate an alternative bidder at the time when an award is made and in the event that a contract is terminated during the execution thereof, the CCT may consider the award of the contract, or non-award, to the alternative bidder in terms of the procedures included its SCM Policy.

2.3.13   Prepare contract documents

2.3.13.1   If necessary, revise documents that shall form part of the contract and that were issued by the CCT as part of the tender documents to take account of:

(a) notices issued during the tender period,
(b) inclusion of some of the returnable documents, and
(c) other revisions agreed between the CCT and the successful tenderer

2.3.13.2   Complete the schedule of deviations attached to the form of offer and acceptance, if any.

2.3.14   **Notice to successful and unsuccessful tenderers**

2.3.14.1   Before accepting the tender of the successful tenderer the CCT shall notify the successful tenderer in writing of the decision of the CCT's Bid Adjudication Committee to award the tender to the successful tenderer. No rights shall accrue to the successful tenderer in terms of this notice

2.3.14.2   The CCT shall, at the same time as notifying the successful tenderer of the Bid Adjudication Committee's decision to award the tender to the successful tenderer, also give written notice to the other tenderers informing them that they have been unsuccessful.

2.3.15   **Provide written reasons for actions taken**

Provide upon request written reasons to tenderers for any action that is taken in applying these Conditions of Tender, but withhold information which is not in the public interest to be divulged, which is considered to prejudice the legitimate commercial interests of tenderers or might prejudice fair competition between tenderers.

TENDER DOCUMENT GOODS AND SERVICES	
SUPPLY CHAIN MANAGEMENT	
SCM - 542	Approved by Branch Manager: 03/04/2020	Version: 8	Page 26 of 66

TENDER NO:	**41S/2022/23**
TENDER DESCRIPTION:	**SUPPLY, INSTALLATION, SERVICE AND MAINTENANCE OF A RECORDS MANAGEMENT DOCUMENT MANANGEMENT AND CASE MANAGEMENT (RM&DM&CM) SOLUTION FOR THE CITY OF CAPE TOWN**
CONTRACT PERIOD:	**FROM DATE OF COMMENCEMENT OF CONTRACT UNTIL 31 MAY 2033**

VOLUME 2: RETURNABLE DOCUMENTS

TENDERER	
NAME of Company/Close Corporation or Partnership / Joint Venture/ Consortium or Sole Proprietor /Individual	
TRADING AS (if different from above)	

NATURE OF TENDER OFFER (please indicate below)	
Main Offer (see clause 2.2.11.1)	
Alternative Offer (see clause 2.2.11.1)	

VOLUME 2: RETURNABLE DOCUMENTS
(3) DETAILS OF TENDERER

1.1 Type of Entity   (Please tick one box)

☐ Individual / Sole Proprietor   ☐ Close Corporation   ☐ Company

☐ Partnership or Joint Venture or Consortium   ☐ Trust   ☐ Other: **………......……….…………**

1.2 Required Details (Please provide applicable details in full):

Name of Company / Close Corporation or Partnership / Joint Venture / Consortium or Individual /Sole Proprietor	
Trading as (if different from above)	
Company / Close Corporation registration number (if applicable)	
Postal address	Postal Code _____
Physical address **(Chosen domicilium citandi et executandi)**	Postal Code _____
Contact details of the person duly authorised to represent the tenderer	Name: Mr/Ms _____ (Name & Surname) Telephone:(_____) _____ Fax:(_____) _____ Cellular Telephone:_____ E-mail address:_____
Income tax number	
VAT registration number	
SARS Tax Compliance Status PIN	
City of Cape Town Supplier Database Registration Number (See Conditions of Tender)	
National Treasury Central Supplier Database registration number (See Conditions of Tender)	

Is tenderer the accredited representative in South Africa for the Goods / Services / Works offered?	☐Yes ☐No If yes, enclose proof
Is tenderer a foreign based supplier for the Goods / Services / Works offered?	☐Yes ☐No If yes, answer the Questionnaire to Bidding Foreign Suppliers (below)
Questionnaire to Bidding Foreign Suppliers	a) Is the tenderer a resident of the Republic of South Africa or an entity registered in South Africa? ☐Yes ☐No
	b) Is the tenderer a resident of the Republic of South Africa or an entity registered in South Africa? ☐Yes ☐No
	c) Does the tenderer have a permanent establishment in the Republic of South Africa? ☐Yes ☐No
	d) Does the tenderer have any source of income in the Republic of South Africa? ☐Yes ☐No
	e) Is the tenderer liable in the Republic of South Africa for any form of taxation? ☐Yes ☐No
Other Required registration numbers	

(4) FORM OF OFFER AND ACCEPTANCE

TENDER NUMBER: 41S/2022/23 - SUPPLY, INSTALLATION, SERVICE AND MAINTENANCE OF A RECORDS MANAGEMENT DOCUMENT MANANGEMENT AND CASE MANAGEMENT (RM&DM&CM) SOLUTION FOR THE CITY OF CAPE TOWN

OFFER: (TO BE FILLED IN BY TENDERER):

Required Details (Please provide applicable details in full):

Name of Tendering Entity* **("the tenderer")**	
Trading as (if different from above)	

AND WHO IS represented herein by: (full names of signatory) _____

duly authorised to act on behalf of the tenderer in his capacity as: (title/ designation) _____

HEREBY AGREES THAT by signing the *Form of Offer and Acceptance,* the tenderer:
1. confirms that it has examined the documents listed in the Index (including Schedules and Annexures) and has accepted all the Conditions of Tender;

2. confirms that it has received and incorporated any and all notices issued to tenderers issued by the CCT;
     6.
3. confirms that it has satisfied itself as to the correctness and validity of the tender offer; that the price(s) and rate(s) offered cover all the goods and/or services specified in the tender documents; that the price(s) and rate(s) cover all its obligations and accepts that any mistakes regarding price(s), rate(s) and calculations will be at its own risk;

4. offers to supply all or any of the goods and/or render all or any of the services described in the tender document to the CCT in accordance with the:
    4.1 terms and conditions stipulated in this tender document;
    4.2 specifications stipulated in this tender document; and
    4.3 at the prices as set out in the **Price Schedule**.

5. accepts full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on it in terms of the Contract.

_____
Signature(s)

_____
Print name(s):
On behalf of the tenderer (duly authorised)

_____
Date

INITIALS OF CITY OFFICIALS		
1	**2**	**3**

FORM OF OFFER AND ACCEPTANCE (continued)

TENDER NUMBER: 41S/2022/23 - SUPPLY, INSTALLATION, SERVICE AND MAINTENANCE OF A RECORDS MANAGEMENT DOCUMENT MANANGEMENT AND CASE MANAGEMENT (RM&DM&CM) SOLUTION FOR THE CITY OF CAPE TOWN

ACCEPTANCE (TO BE FILLED IN BY THE CITY OF CAPE TOWN)

By signing this part of this form of offer and acceptance, the employer identified below accepts the tenderer's offer. In consideration thereof, the employer shall pay the supplier the amount due in accordance with the conditions of contract. Acceptance of the tenderer's offer shall form an agreement between the employer and the tenderer upon the terms and conditions contained in this agreement and in the contract that is the subject of this agreement.

The terms of the contract are contained in:

    (7) & (8):   Special and General Conditions of Tender
    (5):   Price schedule
    (13):   Specifications

and drawings and documents or parts thereof, which may be incorporated by reference into the above listed Parts.

Deviations from and amendments to the documents listed in the tender data and any addenda thereto as listed in the returnable schedules as well as any changes to the terms of the offer agreed by the tenderer and the employer during this process of offer and acceptance, are contained in the schedule of deviations attached to and forming part of this form of offer and acceptance. No amendments to or deviations from said documents are valid unless contained in this schedule.

The tenderer shall within two weeks after receiving a completed copy of this agreement, including the schedule of deviations (if any), contact the employer to arrange the delivery of any securities, bonds, guarantees, proof of insurance and any other documents to be provided in terms of the conditions of contract identified in the special contract conditions. Failure to fulfil any of these obligations in accordance with those terms shall constitute a repudiation of this agreement.

Notwithstanding anything contained herein, this agreement comes into effect on the date when the parties have signed the table below and confirms receipt from the employer of one fully completed original copy of this agreement, including the schedule of deviations (if any). The tenderer (now supplier) shall within five working days of the agreement coming into effect notify the employer in writing of any reason why he cannot accept the contents of this agreement as a complete and accurate memorandum thereof, failing which the agreement presented to the contractor shall constitute the binding contract between the parties.

The Parties	Employer	Supplier
Business Name		
Business Registration		
Tax number (VAT)		
Physical Address		
Accepted contract sum including tax		

The Parties	Employer	Supplier
Accepted contract duration	31	
Signed – who by signature hereto warrants authority		
Name of signatory		
Signed: Date		
Signed: Location		
Signed: Witness		
Name of Witness		

The Parties	Employer	Supplier

FORM OF OFFER AND ACCEPTANCE (continued)
(TO BE FILLED IN BY THE CITY OF CAPE TOWN)

Schedule of Deviations

Notes:
1.   The extent of deviations from the tender documents issued by the CCT before the tender closing date is limited to those permitted in terms of the conditions of tender.
2.   A tenderer's covering letter shall not be included in the final contract document. Should any matter in such letter, which constitutes a deviation as aforesaid, become the subject of agreements reached during the process of offer and acceptance, the outcome of such agreement shall be recorded here.
3.   Any other matter arising from the process of offer and acceptance either as a confirmation, clarification or change to the tender documents and which it is agreed by the Parties becomes an obligation of the contract shall also be recorded here.
4.   Any change or addition to the tender documents arising from the above agreements and recorded here, shall also be incorporated into the final draft of the Contract.

1 Subject . . . .

   Details . . . .

      . . . .

      . . . .

      . . . .

2 Subject . . . .

   Details . . . .

      . . . .

      . . . .

      . . . .

3 Subject . . . .

   Details . . . .

      . . . .

      . . . .

      . . . .

4 Subject . . . .

   Details . . . .

      . . . .

      . . . .

      . . . .

By the duly authorised representatives signing this agreement, the CCT and the tenderer agree to and accept the foregoing schedule of deviations as the only deviations from and amendments to this tender document and addenda thereto as listed in the returnable schedules, as well as any confirmation, clarification or changes to the terms of the offer agreed by the tenderer and the CCT during this process of offer and acceptance.

It is expressly agreed that no other matter whether in writing, oral communication or implied during the period between the issue of the tender documents and the receipt by the tenderer of a completed signed copy of this Agreement shall have any meaning or effect in the contract between the parties arising from this agreement.

(5) PRICE SCHEDULE

Bid specifications may not make any reference to any particular trade mark, name, patent, design, type, specific origin or producer, unless there is no other sufficiently precise or intelligible way of describing the characteristics of the work, in which case such reference must be accompanied by the words "or equivalent".

TENDERERS MUST NOTE THAT WHEREVER THIS DOCUMENT REFERS TO ANY PARTICULAR TRADE MARK, NAME, PATENT, DESIGN, TYPE, SPECIFIC ORIGIN OR PRODUCER, SUCH REFERENCE SHALL BE DEEMED TO BE ACCOMPANIED BY THE WORDS 'OR EQUIVALENT"

Pricing Instructions:

5.1   State the rates and prices in Rand unless instructed otherwise in the tender conditions.

5.2   Include in the rates, prices, and the tendered total of the prices (if any) all duties, taxes (except Value Added Tax (VAT), and other levies payable by the successful tenderer, such duties, taxes and levies being those applicable 14 days before the closing time stated in the General Tender Information.

5.3   All prices tendered must include all expenses, disbursements and costs (e.g., transport, accommodation etc.) that may be required for the execution of the tenderer's obligations in terms of the Contract, and shall cover the cost of all general risks, liabilities and obligations set forth or implied in the Contract as well as overhead charges and profit (in the event that the tender is successful). All prices tendered will be final and binding.

5.4   All prices shall be tendered in accordance with the units specified in this schedule.

5.5   Where a value is given in the Quantity column, a Rate and Price (the product of the Quantity and Rate) is required to be inserted in the relevant columns.

5.6   The successful tenderer is required to perform all tasks listed against each item per schedule tendered for. The tenderer must therefore tender prices/rates on all items as per the section in the Price Schedule. **An item against which no rate is/are entered, or if anything other than a rate or a nil rate (for example, a zero, a dash or the word "included" or abbreviations thereof) is entered against an item, it will also be regarded as a nil rate having been entered against that item, i.e., that there is no charge for that item. The Tenderer may be requested to clarify nil rates, or items regarded as having nil rates; and the Employer may also perform a risk analysis with regard to the reasonableness of such rates.**

5.7   Provide fixed rates and prices for the duration of the contract that are not subject to adjustment except as otherwise provided for in clause 17 of the Conditions of Contract and as amplified in the Special Conditions of Contract. If a forward cover rate is applied for any price variations, such rates must be made available to the CCT in this tender.

5.8   General specifications for items in the (5) Price Schedule, appear in section (13) SPECIFICATION(S). Tenderers must refer to these specifications when completing the Price Schedule.

5.9   **Mark-up percentage (%)** is the method where an all-inclusive mark-up percentage (%) is applied to the discounted (if any Discount Offered (%) Recommended Retail Price List [RRPL] of the Original Software Manufacturer(s) [OSM].

      o   **Mark-up percentage (%)** is the mark-up amount expressed as a percentage (%) of the discounted OSM Recommended Retail Price by applying the formula:
          ▪   Mark-up % = (Mark-up amount / discounted OSM RR Price) × 100

      o   **Unconditional Discount Offered (%)** is the discount amount expressed as a percentage (%) of the OSM Recommended Retail Price by applying the formula:
          ▪   Discount % = (Discount amount / OSM Price) × 100

      o   **Evaluation Price** – This is the price that will be invoiced to the City and is calculated by the formula below and used for the tender price evaluation based on the ranking of tender prices from lowest to highest price. PLEASE NOTE – Discounts offered with conditions cannot be considered for evaluation and is such case the formula below will not include subtraction of

the discount. Tenders must therefore clearly indicate if discounts offered on the OSM price are unconditional:

- Evaluation Price = OSM Price + Mark up - Discount Offered.

5.10 The tenderer shall provide detailed and comprehensive OSM Recommended Retail Price Lists, for each OSM listed in the Price Schedules, in support of their Bid. The OSM price is the Original Equipment Manufacture's Recommended Retail Price at the closing date of the tender. CCT reserves the right to approach the Original Software Manufacturer directly for OSM Recommended Retail Price Lists, if required; for verification purposes.

5.11 Schedules A, B, C, D and E will be grouped and awarded collectively/ in its entirety. Tenderers must therefore price for all Schedules and items within the schedules.

5.13   The mark-up %'s tendered for Schedule A of the Price Schedule will be fixed for the duration of the contract. For each purchase order, a quotation must be submitted by the service provider which must be accompanied by an updated Original Equipment Manufacturer (OSM) in order for the City to verify the purchase order price (OSM price plus mark-up and unconditional discount if applicable) charged by the service provider.

The rates tendered for Schedules C, D, E and F of the Price Schedule will be subject to contract price adjustment in terms of Consumer Price Index (CPI), as referred to in Schedule 8.

INITIALS OF CITY OFFICIALS		
1	2	3

SCHEDULE A. SUPPLY OF THE RM&DM&CM SOLUTION - SUPPLY OF SOFTWARE AND LICENCING FOR THE RM&DM&CM SOLUTION

TABLE A.1. SUPPLY OF THE RM&DM&CM SOLUTION
This table is for the pricing to supply an OSM product for the RM&DM&CM solution
Tenderers must identify the software OSM or vendor in the indicated column (column 3). **Refer to section (13) 13.4 Specifications and relevant paragraphs describing the functional and non-functional requirements**
Refer to section (13) 13.7 Specifications for detail specifications of the maintenance requirements.
Tenderers must identify the software OSM or vendor in the indicated column (column 3).
Tenders are reminded to complete Schedule 15G and attach to Schedule 15H the OSM Recommended Retail Price List where the OSM Price List is requested to be submitted together with the tender response.

Item	Description	Source of Goods Identify OSM or Distributor	Unit of Measure	Mark-Up (%)	Discount (%)	OSM Price per Unit (Excl. VAT)
A.1.1.	RM&DM&CM Software Solution ((The once off price to procure the software application / application suite))		Per Software Application / Application Suite	%	%	R
A.1.2.	Recurring Software Licence Price (This would be the price per user or transaction or per client access or per usage volume.)		Please indicate the unit of measure.	%	%	R
A.1.3.	Software Maintenance (Software bug fixes, software / security patches, new features, software updates/upgrades.)		Per Year	%	%	

Note:

1. Tenderers are to submit pricing for either A1.1, A.1.2 or both A1.1 and A.1.2; depending on the solution offered.

2. If either A.1.1 or A.1.2 is not applicable to the solution offered, tenderers are to indicate "N/A" in the last column.

3. For or A.1.3 if software maintenance is offered with a different frequency, tenderers must calculate the annual price as per the unit of measure which is "per year"

SCHEDULE B. PILOT TEST PROJECT – PRICING FOR THE IMPLEMENTATION OF A PILOT PROJECT

TABLE B.1. IMPLEMENTATION OF A PILOT PROJECT			
This table is for the pricing to conduct a pilot project implementation for the RM&DM&CM SOLUTION. Tenderers **must refer to point 34 in SECTION 7 of the SPECIAL CONDITIONS OF CONTRACT as well as SECTION (13) 13.4.5** Specifications and relevant paragraphs describing the Pilot Project requirements			

Item	Description	Unit	Price per Unit (Excl. VAT)
B.1.1.	Pilot 1	Implementation and Migration	R
B.1.2.	Pilot 2	Implementation and Migration	R
B.1.3.	Pilot 3	Implementation and Migration	R
B.1.4.	Provision of a Technical Analysis Report for DAMS Functionality	Complete Report	R

SCHEDULE C. PROVISION OF ONCE-OFF SERVICES FOR INSTALLATION IMPLEMENTATION AND MIGRATION OF THE RM&DM&CM SOLUTION

TABLE C.1. INSTALLATION IMPLEMENTATION AND MIGRATION OF THE RM&DM&CM SOLUTION
This table is for the pricing of services to install, Implement and Migrate existing solutions and content to the proposed OSM solution for the proposed RM&DM&CM Solution
Refer to section (13) Specifications, with a focus on 13.5.6 and relevant paragraphs describing the implementation and migration requirements.
Tenderers are reminded to complete the Schedules 15B, 15C, 15D, 15E and 15F, and attach to Schedule 15H the OSM Recommended Retail Price List and Schedule 15J the detailed project plan

Item	Description	Unit	Price per Unit (Excl. VAT)
C.1.1.	Installation of the RM&DM&CM Solution, according to the requirements, project methodology and deliverables as described in section **(13) Specifications (13.5)**	Complete Installation	R
C.1.2.	Migration and implementation of **SharePoint** according to the implementation requirements, project methodology and deliverables as described in section **(13) Specifications (13.5)**	Complete Implementation and Migration	R
C.1.3.	Migration and implementation of **SAP Records and Case Management (SAP RCM)** according to the implementation requirements, project methodology and deliverables as described in section **(13) Specifications (13.5)**	Complete Implementation and Migration	R
C.1.4.	Migration and implementation of **FS01 (File server)** according to the implementation requirements, project methodology and deliverables as described in section **(13) Specifications (13.5)**	Complete Implementation and Migration	R

SCHEDULE D. PROVISION OF SUPPORT SERVICES

TABLE D.1. SUPPORT SERVICES
This table is for the pricing of maintenance and support services for the RM&DM&CM SOLUTION. **Refer to section (13) 13.7 Specifications for detail specifications of the maintenance and support requirements.** **Tenders are reminded to complete the Schedules 15B, 15C, 15D, 15E and 15F, and attach to Schedule 15H the OSM Recommended Retail Price List.**

Item	Description	Unit	Price per Unit (Excl. VAT)
D.1.1.	Adhoc Support Services	Per incident	R

SCHEDULE E. PROVISION OF TRAINING SERVICES FOR THE RM&DM&CM SOLUTION

	TABLE E.1. PROVISION OF TRAINING SERVICES FOR THE RM&DM&CM SOLUTION		
	This table is for the pricing of training services for proposed OSM solution for the proposed RM&DM&CM Solution.		
	Refer to section (13) 13.6 Specifications and relevant paragraphs describing the training requirements.		
	Tenders are reminded to complete the Schedules 15B, 15C, 15D, 15E and 15F, and attach to Schedule 15H the OSM Recommended Retail Price List.		

Item	**Description**	**Unit**	**Price**
E.1.1.	Train the trainer Training to be provided according to requirements, and deliverables as described in section **(13) Specifications (13.6)**		
E.1.1.1.	Train the trainer: 1 to 10 Trainees (Classroom based training)	Per User / Trainer	R
E.1.1.2.	Train the trainer: 1 to 10 Trainees (Virtual training)	Per User / Trainer	R
E.1.2.	System Admin Training Training to be provided according to requirements, and deliverables as described in section **(13) Specifications (13.6)**		
E.1.2.1.	System Admin Training: 1 to 10 Trainees (Classroom based training)	Per User / Trainer	R
E.1.2.2.	System Admin Training: 1 to 10 Trainees (Virtual training)	Per User / Trainer	R
E.1.3.	Business Admin Training Training to be provided according to requirements, and deliverables as described in section **(13) Specifications (13.6)**		
E.1.3.1.	Business Admin: 1 to 10 Trainees (Classroom based training)	Per User / Trainer	R
E.1.3.2.	Business Admin Training: 1 to 10 Trainees (Virtual training)	Per User / Trainer	R
E.1.4.	Power User Training Training to be provided according to requirements, and deliverables as described in section **(13) Specifications (13.6)**		
E.1.4.1.	Power User Training: 1 to 10 Trainees (Classroom based training)	Per User / Trainer	R
E.1.4.2.	Power User Training: 1 to 10 Trainees (Virtual training)	Per User / Trainer	R

PROVISION OF PROFESSIONAL SERVICES FOR THE RM&DM&CM SOLUTION

TABLE E.2. PROFESSIONAL SERVICES FOR THE RM&DM&CM SOLUTION
This table is for the labour rates associated with the ad-hoc Services for the RM&DM&CM Solution.
Refer to section (13) 13.8 Specifications and relevant paragraphs describing Professional Services Requirements
Tenderers are required to respond with the fixed rates for the duration of the contract for all services. Note rates are fixed, as the tender conditions do not allow for contract price adjustments. Failure to complete each category of the pricing schedule will render the tender non-responsive. Fill in the costing table as provided below.
Tenders are reminded to complete the Schedules 15B, 15C, 15D, 15E and 15F, and attach to Schedule 15H the OSM Recommended Retail Price List.

Item	Description	Unit	Price per Unit (ZAR excl. VAT)
E.2.1.	RM& DM Project Manager	per hour	R
E.2.2.	RM&DM&CM Software Developer	per hour	R
E.2.3.	RM&DM&CM Technical Lead	per hour	R
E.2.4.	RM&DM&CM Technical Consultant	per hour	R

(6) SUPPORTING SCHEDULES

Schedule 1: Certificate of Authority for Partnerships/ Joint Ventures/ Consortiums

This schedule is to be completed if the tender is submitted by a partnership/joint venture/ consortium.

1. We, the undersigned, are submitting this tender offer as a partnership/ joint venture/ consortium and hereby authorize Mr/Ms _____, of the authorised entity _____, acting in the capacity of Lead Partner, to sign all documents in connection with the tender offer and any contract resulting from it on the partnership/joint venture/ consortium's behalf.

2. By signing this schedule, the partners to the partnership/joint venture/ consortium:

    2.1 warrant that the tender submitted is in accordance with the main business and objectives of the partnership/joint venture/ consortium;

    2.2 agree that the CCT shall make all payments in terms of this Contract into the following bank account of the Lead Partner:

    Account Holder: _____

    Financial Institution: _____

    Branch Code: _____

    Account No.: _____

    2.3 agree that in the event that there is a change in the partnership/ joint venture/ consortium and/or should a dispute arise between the partnership/joint venture/ consortium partners, that the CCT shall continue to make any/all payments due and payable in terms of the Contract into the aforesaid bank account until such time as the CCT is presented with a Court Order or an original agreement (signed by each and every partner of the partnership/joint venture/ consortium) notifying the CCT of the details of the new bank account into which it is required to make payment.

    2.4 agree that they shall be jointly and severally liable to the CCT for the due and proper fulfilment by the successful tenderer/supplier of its obligations in terms of the Contract as well as any damages suffered by the CCT as a result of breach by the successful tenderer/supplier. The partnership/joint venture/ consortium partners hereby renounce the benefits of excursion and division.

SIGNED BY THE PARTNERS OF THE PARTNERSHIP/ JOINT VENTURE/ CONSORTIUM		
NAME OF FIRM	ADDRESS	DULY AUTHORISED SIGNATORY
Lead partner		Signature…………………………….... Name………………………………… Designation…………………………...
		Signature…………………………….... Name………………………………… Designation…………………………...
		Signature…………………………….... Name………………………………… Designation…………………………...
		Signature…………………………….... Name………………………………… Designation…………………………...

Note: A copy of the Joint Venture Agreement shall be appended to List of other documents attached by tenderer schedule**.**

Schedule 2: Declaration for Procurement above R10 million

If the value of the transaction is expected to exceed R10 million (VAT included) the tenderer shall complete the following questionnaire, attach the necessary documents and sign this schedule:

1.   Are you by law required to prepare annual financial statements for auditing? (Please mark with X)

YES		NO	

   1.1   If YES, submit audited annual financial statements:

   (i)   for the past three years, or
   (ii)   since the date of establishment of the tenderer (if established during the past three years)

   By attaching such audited financial statements to **List of other documents attached by tenderer** schedule.

2.   Do you have any outstanding undisputed commitments for municipal services towards the CCT or other municipality in respect of which payment is overdue for more than 30 (thirty) days? (Please mark with X)

YES		NO	

   2.1   If NO, this serves to certify that the tenderer has no undisputed commitments for municipal services towards any municipality for more than three (3) (three) months in respect of which payment is overdue for more than 30 (thirty) days.

   2.2   If YES, provide particulars:

   _____
   _____
   _____
   _____

3.   Has any contract been awarded to you by an organ of state during the past five (5) years? (Please mark with X)

YES		NO	

3.1   If YES, insert particulars in the table below including particulars of any material non-compliance or dispute concerning the execution of such contract. Alternatively attach the particulars to **List of other documents attached by tenderer** schedule in the same format as the table below:

Organ of State	Contract Description	Contract Period	Non-compliance/dispute (if any)

4.   Will any portion of the goods or services be sourced from outside the Republic, and if so, what portion and whether any portion of payment from the CCT is expected to be transferred out of the Republic? (Please mark with X)

YES		NO	

4.1   If YES, furnish particulars below

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the employer of any other remedies available to it.

_____   _____
Signature
Print name: Date
On behalf of the tenderer (duly authorised)

Schedule 3: Preference Schedule

1   Definitions

The following definitions shall apply to this schedule:

All applicable taxes: Includes value-added tax, pay as you earn, income tax, unemployment insurance fund contributions and skills development levies.

Applicable Code: Shall be either the Amended Codes of Good Practise (published on 11 October 2013) or Sector Specific Codes as indicated in the tender conditions

B-BBEE: Broad-based black economic empowerment as defined in section 1 of the Broad-Based Black Economic Empowerment Act.

B-BBEE status level of contributor: The B-BBEE status of an entity in terms of a code of good practice on black economic empowerment issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act

Bid (Tender): A written offer in a prescribed or stipulated form in response to an invitation by an organ of state for the provision of services, works or goods, through price quotations, advertised competitive bidding processes or proposals.

Black Designated Groups: The meaning assigned to it in the codes of good practice issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act, 2003, (Act 53 of 2003).

Black People: The meaning assigned to it in section 1 of the Broad-Based Black Economic Empowerment Act.

Broad-Based Black Economic Empowerment Act: The Broad-Based Black Economic Empowerment Act, Act 53 of 2003.

Consortium or Joint Venture: An association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

Contract The agreement that results from the acceptance of a bid by an organ of state.

Co-operative: A co-operative registered in terms of section 7 of the Co-operatives Act, 2005 (Act no. 14 of 2005).

Designated Group: Black designated groups, black people, women, people with disabilities or small enterprises as defined in section 1 of the National Small Enterprises Act, 1996 (act no. 102 of 1996)

Designated Sector: A sector, sub-sector or industry or product that has been designated in terms of any relevant regulation of the Preferential Procurement Regulations, 2017.

Exempted Micro Enterprise (EME): An exempted micro enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act

Firm Price: The price that is only subject to adjustments in accordance with the actual increase or decrease resulting from the change, imposition, or abolition of customs or excise duty and any other duty, levy, or tax, which, in terms of the law or regulation, is binding on the contractor and demonstrably has an influence on the price of any supplies, or the rendering costs of any service, for the execution of the contract.

Functionality: The ability of a tenderer to provide goods or services in accordance with specifications as set out in the tender documents.

Military Veteran: The meaning assigned to it in section 1 of the Military Veterans Act, 2011 (Act No. 18 of 2011).

National Treasury: The meaning assigned to it in section 1 of the Public Finance Management Act, 1999 (Act No. 18 of 1999.

Non-firm prices: All prices other than "firm" prices.

Person: Includes a juristic person.

People with disabilities: The meaning assigned to it in section 1 of the Employment Equity Act, 1998 (Act No. 55 of 1998).

Price: Includes all applicable taxes less unconditional discounts.

Proof of B-BBEE status level of contributor: The B-BBEE status level certificate issued by an authorised body or person, a sworn affidavit as prescribed by the B-BBEE Codes of good Practice or any other requirement prescribed in terms of the Broad-Based Black Economic Empowerment Act.

Qualifying Small Enterprise (QSE): A qualifying small enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act.

Rand Value: means the total estimated value of a contract in Rand, calculated at the time of bid invitations.

Rural Area: A sparsely populated area in which people farm or depend on natural resources, including villages and small towns that are dispersed through the area or an area including a large settlement which depends on migratory labour and remittances and government social grants for survival, and may have a traditional land tenure system.

Stipulated Minimum Threshold: The minimum threshold stipulated in terms of any relevant regulation of the Preferential Procurement Regulations, 2017.

Sub-contract: The primary contractor's assigning, leasing, making out work to, or employing, another person to support such primary contractor in the execution of part of a project in terms of the contract.

The Act: The Preferential Procurement Policy Framework Act, 2000 (Act No 5 of 2000).

Total Revenue: Bears the same meaning assigned to this expression in the Codes of Good Practice on Black Economic Empowerment, issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act and promulgated in the *Government Gazette* on 9 February 2007.

Township: An urban living area that at any time from the late 19th century until 27 April 1994, was reserved for black people, including areas developed for historically disadvantaged individuals post 27 April 1994.

Treasury: The meaning assigned to it in section 1 of the Public Finance Management Act, 1999 (Act No. 18 of 1999).

Trust: The arrangement through which the property of one person is made over or bequeathed to a trustee to administer such property for the benefit of another person.

Trustee: Any person, including the founder of a trust, to whom property is bequeathed in order for such property to be administered for the benefit of another person.

Youth: The meaning assigned to it in section 1 of the National Youth Development Agency Act, 2008 (Act No. 54 of 2008).

2 Conditions associated with the granting of preferences

A supplier that is granted a preference undertakes to:

1) accept that the number of preference points allocated will be based on the B-BBEE status level of contributor of the supplier as at the closing date for submission of tender offers;

2) not sub-contract more than 25% of the value of the contract to sub-contractors that do not have an equal or higher B-BBEE status level of contributor than the supplier, unless the intended sub-contractors are exempted micro enterprises that have the capability and ability to execute the sub-contract works or unless otherwise declared in terms of Section 5 below;

3) accept that a contract may not be awarded if the price offered is not market related;

4) accept the sanctions set out in Section 3 below should Condition 2(2) be breached, or should the tenderer have submitted any false information regarding its B-BBEE status level of contributor, local production and content, or any other matter required in terms of this bid that will affect, or has affected the bid evaluation;

5) accept that, in order to qualify for preference points, it is the responsibility of the supplier to submit documentary proof of its BBBEE level of contribution in accordance with the Codes of Good Practise, 2013, to the CCT at the Supplier Management Unit located within the Tender Distribution Office, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town (Tel 021 400 9242/3/4/5);

6) accept that, further to 5) above, Consortiums/Joint Ventures will qualify for preference points, provided that the entity submits the relevant certificate/scorecard in terms of the Preferential Procurement Regulations, 2017. Note that, in the case of unincorporated entities, a verified scorecard in the name of the consortium/Joint Venture must be submitted with the quotation (attached to this schedule);

7) accept that if it is found that, in the performance of the contract, the participation of the various partners in a Consortium/ Joint Venture differs substantially from that upon which the consolidated scorecard submitted in terms of 5) above was based, and the impact of which is that the Joint Venture would not have been awarded the contract in terms of the actual B-BBEE level of contribution achieved by the Joint Venture, then a financial penalty shall be applied (in addition to any other remedies that the CCT may have) in accordance with Section 3 below;

8) accept that the CCT will verify the B-BBEE level of contributor of the supplier as at the closing date for submission of tender offers, to determine the number of preference points to be awarded to the supplier.

In the case of Consortiums/Joint Ventures which tender as unincorporated entities, a verified scorecard submitted with the tender and valid as at the closing date will be used to determine the number of preference points to be awarded to the supplier;

9)   accept that, notwithstanding 8) above, a supplier will not be awarded points for B-BBEE status level of contributor if he indicates in his tender that he intends sub-contracting more than 25% of the value of the contract to sub-contractors that do not qualify for at least the points that the supplier qualifies for unless the intended sub-contractors are exempted micro enterprises that have the capability and ability to execute the sub-contract works;

10)   accept that any subcontracting arrangements after the award of the tender may only be entered into upon the prior approval of the City of Cape Town; and

11)   immediately inform the City of Cape Town of any change that may affect the tenderer's B-BBEE level of contribution upon which preference points will be or have been allocated.

3 Sanctions relating to breaches of preference conditions

The sanctions for breaching the conditions associated with the granting of preferences are:

1) disqualify the supplier from the tender process;

2) recover costs, losses or damages the CCT has incurred or suffered as a result of the supplier's or contractor's conduct;

3) cancel the contract in whole or in part and claim any damages which the CCT has suffered as a result of having to make less favourable arrangements due to such cancellation;

4) restrict the supplier, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, from obtaining business from the CCT for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied and inform the National Treasury accordingly;

5) forward the matter for criminal prosecution; and/or

6) financial penalties payable to the CCT, as set out below.

Financial penalty for breach of Condition 2 in Section 2 above:

The penalty to be applied for sub-contracting more than 25% of the value of the contract to sub-contractors that do not qualify for at least the preference points that the supplier qualified for (unless so declared or proven to be beyond the control of the supplier, or the sub-contractors are EMEs that have the capability and ability to execute the sub-contract works) shall be as provided for in the following formula:

Penalty = 0.5 x E(%) x P*

where:

   E = The value of work (excluding VAT) executed by sub-contractors that do not qualify for at least the preference points that the supplier qualified for, expressed as a percentage of P*, less 25%

   P* = Value of the contract

Financial penalty for breach in terms of condition 6 in Section 2 above:

The penalty to be applied where, in the performance of the contract, the participation of the various partners in a Consortium/ Joint Venture differs substantially from that upon which the consolidated scorecard submitted in terms of 5) in Section 2 above was based, and the impact of which is that the Joint Venture would not have been awarded that contract in terms of the actual B-BBEE level of contribution achieved by the Joint Venture, shall be as provided for in the following formula:

Penalty = 5/100 x (B-BBEE^a – B-BBEE^t) x P*

where:

B-BBEE^a =   The B-BBEE level of contribution that is achieved, determined in accordance with the actual participation of the Joint Venture partners in the performance of the contract

B-BBEE^t =   The B-BBEE level of contribution that was used to determine the number of preference points granted to the Joint Venture at the time of tender evaluation

P*   =   Value of the contract

Financial penalty for breach in terms of condition 10 in Section 2 above:

The penalty to be applied where the supplier fails to disclose subcontracting arrangement after the award of the tender is up to a maximum of 10% of the value of the contract.

4 Level of Contribution in respect of enterprise status or structure of the tendering entity (the supplier)

In the interest of transparency, suppliers are required to complete Table 1: Level of Contribution below.

Table 1: Level of Contribution

Type of B-BBEE Contributor	Status (tick box(es) below as applicable)
Exempted Micro Enterprise (EME), 100% black-owned	☐
Exempted Micro Enterprise (EME), at least 51% but less than 100% black-owned	☐
Exempted Micro Enterprise (EME), less than 51% black-owned	☐
Qualifying Small Enterprise (QSE), 100% black-owned	☐
Qualifying Small Enterprise (QSE), at least 51% but less than 100% black-owned	☐
Qualifying Small Enterprise (QSE), less than 51% black-owned	☐
Verified B-BBEE contributor B-BBEE Status Level of Contributor[1] ☐	☐
Non-compliant contributor	☐

[1] If it is indicated that the company/firm/entity is a verified B-BBEE contributor, then the verified status level of contributor must be inserted in the box provided (insert a number from 1 to 8 as applicable)

5 Declarations

1) With reference to Condition 8 in Section 2 above, the supplier declares that:

> **I/we hereby forfeit my preference points because I /we DO intend sub-contracting more than 25% of the value of the contract to sub-contractors that do not qualify for at least the points that I/we as supplier qualify for or are not exempted micro enterprises that have the capability and ability to execute the sub-contract works**

☐

Note:

Suppliers who do not tick this box will be allocated preference points but the sanctions relating to breaches of preference conditions in Section 3 will be applicable if the supplier contravenes the conditions in Section 2.

2) The undersigned, who warrants that he/she is duly authorised to do so on behalf of the supplier, hereby certifies that the preference claimed based on the B-BBEE status level of contribution indicated in Table 1, qualifies the supplier, subject to condition 8 in Section 2 above, for such preference claimed, and acknowledges that:

   (i)   the information furnished is true and correct;

   (ii) the preference claimed is in accordance with the conditions of this schedule;

   (iii) the supplier may be required to furnish documentary proof to the satisfaction of the CCT that the BBBEE level of contributor as at the closing date is correct; and

   iv)   he/she understands the conditions under which preferences are granted, and confirms that the supplier will satisfy the conditions pertaining to the granting of preferences.

_____   _____

Signature   **Date**

_____

Name (PRINT)

(For and on behalf of the Supplier (duly authorised))

For official use.		
SIGNATURE OF CITY OFFICIALS AT TENDER OPENING		
1.	**2.**	**3.**

Schedule 4: Declaration of Interest – State Employees (MBD 4 amended)

1. No bid will be accepted from:
    1.1 persons in the service of the state[1], or
    1.2 if the person is not a natural person, of which any director, manager or principal shareholder or stakeholder is in the service of the state, or
    1.3 from persons, or entities of which any director, manager or principal shareholder or stakeholder, has been in the service of the City of Cape Town during the twelve months after the City employee has left the employ of the City, or
    1.4 from an entity who has employed a former City employee who was at a level of T14 of higher at the time of leaving the City's employ and involved in any of the City's bid committees for the bid submitted, if:
        1.4.1 the City employee left the City's employment voluntarily, during a period of 12 months after the City employee has left the employ of the City;
        1.4.2 the City employee left the City's employment whilst facing disciplinary action by the City, during a period of 24 months after the City employee has left the employ of the City, or any other period prescribed by applicable legislative provisions, after having left the City's employ.

2. Any person, having a kinship with persons in the service of the state, including a blood relationship, may make an offer or offers in terms of this invitation to bid. In view of possible allegations of favouritism, should the resulting bid, or part thereof, be awarded to persons connected with or related to persons in service of the state, it is required that the tenderer or their authorised representative declare their position in relation to the evaluating/adjudicating authority.

3. In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.

    3.1 Full Name of tenderer or his or her representative:……………………………………………...
    .2 Identity Number:……………………………………………………………………………………

    3.3 Position occupied in the Company (director, trustee, shareholder[2])………………………

    3.4 Company or Close Corporation Registration Number:………………………………………

    3.5 Tax Reference Number……………………………………………………………………………..

    3.6 VAT Registration Number:……………………………………………………………………………

    3.7 The names of all directors / trustees / shareholders members, their individual identity numbers and state employee numbers must be indicated in paragraph 4 below.

    3.8 Are you presently in the service of the state? **YES / NO**

        3.8.1 If yes, furnish particulars …………………………………………………………………….

    3.9 Have you been in the service of the state for the past twelve months? **YES / NO**

        3.9.1 If yes, furnish particulars …………………………………………………………………

    3.10 Do you have any relationship (family, friend, other) with persons in the service of the state and who may be involved with the evaluation and or adjudication of this bid? **YES / NO**

        3.10.1 If yes, furnish particulars ………………………………………………………………………

    3.11 Are you, aware of any relationship (family, friend, other) between any other tenderer and any persons in the service of the state who may be involved with the evaluation and or adjudication of this bid? **YES / NO**

        3.11.1 If yes, furnish particulars……………………………………………………………………

    3.12 Are any of the company's directors, trustees, managers, principle shareholders or stakeholders in service of the state? **YES / NO**

        3.12.1 If yes, furnish particulars ………………………………………………………………..…

3.13   Are any spouse, child or parent of the company's directors, trustees, managers, principle shareholders or stakeholders in service of the state? **YES / NO**

      3.13.1 If yes, furnish particulars ……………………………………………………………………

3.14   Do you or any of the directors, trustees, managers, principle shareholders, or stakeholders of this company have any interest in any other related companies or business whether or not they are bidding for this contract?   **YES / NO**

      3.14.1 If yes, furnish particulars …………………………………………………………………………

3.15   Have you, or any of the directors, trustees, managers, principle shareholders, or stakeholders of this company been in the service of the City of Cape Town in the past twelve months?   **YES / NO**

      3.15.1 If yes, furnish particulars …………………………………………………………………………

3.16   Do you have any employees who was in the service of the City of Cape Town at a level of T14 or higher at the time they left the employ of the City, and who was involved in any of the City's bid committees for this bid?   **YES / NO**

      3.16.1 If yes, furnish particulars …………………………………………………………………………

4.   Full details of directors / trustees / members / shareholders

Full Name	Identity Number	State Employee Number

If the above table does not sufficient to provide the details of all directors / trustees / shareholders, please append full details to the tender submission.

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the employer of any other remedies available to it.

_____   _____
Signature
Print name: Date
On behalf of the tenderer (duly authorised)

¹MSCM Regulations: "in the service of the state" means to be –

(a) *a member of –*
    (i)   *any municipal council;*
    (ii)   *any provincial legislature; or*
    (iii)   *the national Assembly or the national Council of provinces;*

(b) *a member of the board of directors of any municipal entity;*
(c) *an official of any municipality or municipal entity;*
(d) *an employee of any national or provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act No.1 of 1999);*
(e) *an executive member of the accounting authority of any national or provincial public entity; or*
(f) *an employee of Parliament or a provincial legislature.*

² Shareholder" means a person who owns shares in the company and is actively involved in the management of the company or business and exercises control over the company.

Schedule 5: Conflict of Interest Declaration

1.   The tenderer shall declare whether it has any conflict of interest in the transaction for which the tender is submitted. (Please mark with X)

YES		NO	

      1.1   If yes, the tenderer is required to set out the particulars in the table below:

2.   The tenderer shall declare whether it has directly or through a representative or intermediary promised, offered or granted:

      2.1   any inducement or reward to the CCT for or in connection with the award of this contract; or

      2.2   any reward, gift, favour or hospitality to any official or any other role player involved in the implementation of the supply chain management policy. (Please mark with X)

YES		NO	

If yes, the tenderer is required to set out the particulars in the table below:

Should the tenderer be aware of any corrupt or fraudulent transactions relating to the procurement process of the City of Cape Town, please contact the following:

the City's anti-corruption hotline at 0800 32 31 30 (toll free)

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the employer of any other remedies available to it.

_____   _____
Signature
Print name: Date
On behalf of the tenderer (duly authorised)

Schedule 6: Declaration of Tenderer's Past Supply Chain Management Practices (MBD 8)

Where the entity tendering is a partnership/joint venture/consortium, each party to the partnership/joint venture/consortium must sign a declaration in terms of the Municipal Finance Management Act, Act 56 0f 2003, and attach it to this schedule.

1   The tender offer of any tenderer may be rejected if that tenderer or any of its directors/members have:

  a) abused the municipality's / municipal entity's supply chain management system or committed any fraudulent conduct in relation to such system;
  b) been convicted for fraud or corruption during the past five years;
  c) willfully neglected, reneged on or failed to comply with any government, municipal or other public sector contract during the past five years; or
  d) been listed in the Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No 12 of 2004) or Database of Restricted Suppliers.

2   In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.

Item	Question	Yes	No
2.1	**Is the tenderer or any of its directors/members listed on the National Treasury's Database of Restricted Suppliers as companies or persons prohibited from doing business with the public sector?** (Companies or persons who are listed on this Database were informed in writing of this restriction by the Accounting Officer/Authority of the institution that imposed the restriction after the *audi alteram partem* rule was applied). **The Database of Restricted Suppliers now resides on the National Treasury's website(www.treasury.gov.za) and can be accessed by clicking on its link at the bottom of the home page.**	Yes ☐	No ☐
2.1.1	If so, furnish particulars:		
2.2	Is the tenderer or any of its directors/members listed on the Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No 12 of 2004) or Database of Restricted Suppliers? **The Register for Tender Defaulters can be accessed on the National Treasury's website (www.treasury.gov.za) by clicking on its link at the bottom of the home page.**	Yes ☐	No ☐
2.2.1	If so, furnish particulars:		
2.3	Was the tenderer or any of its directors/members convicted by a court of law (including a court of law outside the Republic of South Africa) for fraud or corruption during the past five years?	Yes ☐	No ☐

2.3.1	If so, furnish particulars:		

Item	Question	Yes	No
2.4	Does the tenderer or any of its directors owe any municipal rates and taxes or municipal charges to the municipality / municipal entity, or to any other municipality / municipal entity, that is in arrears for more than three months?	Yes ☐	No ☐
2.4.1	If so, furnish particulars:		
2.5	Was any contract between the tenderer and the municipality / municipal entity or any other organ of state terminated during the past five years on account of failure to perform on or comply with the contract?	Yes ☐	No ☐
2.7.1	If so, furnish particulars:		

The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, , restriction of the tenderer or the exercise by the employer of any other remedies available to it.

_____   _____

Signature
Print name: Date
On behalf of the tenderer (duly authorised)

Schedule 7: Authorisation for the Deduction of Outstanding Amounts Owed to the City of Cape Town

To: THE CITY MANAGER, CITY OF CAPE TOWN

From: _____
        (Name of tenderer)

RE: AUTHORISATION FOR THE DEDUCTION OF OUTSTANDING AMOUNTS OWED TO THE CITY OF CAPE TOWN

The tenderer:

a) hereby acknowledges that according to SCM Regulation 38(1)(d)(i) the City Manager may reject the tender of the tenderer if any municipal rates and taxes or municipal service charges owed by the tenderer (or any of its directors/members/partners) to the CCT, or to any other municipality or municipal entity, are in arrears for more than 3 (three) months; and

b) therefore hereby agrees and authorises the CCT to deduct the full amount outstanding by the Tenderer or any of its directors/members/partners from any payment due to the tenderer; and

c) confirms the information as set out in the tables below for the purpose of giving effect to b) above;

d) The tenderer hereby certifies that the information set out in this schedule and/or attached hereto is true and correct, and acknowledges that failure to properly and truthfully complete this schedule may result in steps being taken against the tenderer, the tender being disqualified, and/or (in the event that the tenderer is successful) the cancellation of the contract, restriction of the tenderer or the exercise by the employer of any other remedies available to it.

Physical **Business** address(es) of the tenderer	Municipal Account number(s)

If there is not enough space for all the names, please attach the information to **List of other documents attached by tenderer** schedule in the same format:

Name of Director / Member / Partner	Identity Number	Physical **residential** address of Director / Member / Partner	Municipal Account number(s)

_____   _____
Signature
Print name: Date
On behalf of the tenderer (duly authorised)

Schedule 8: Contract Price Adjustment and/or Rate of Exchange Variation

Pricing Instructions:

8.1 The %'s tendered for Schedules A of the Price Schedule will be fixed for the duration of the contract.

8.2 The rates tendered for Scheduled B, C, D, E and F of the Price Schedule will be subject to contract price adjustment in terms of Consumer Price Index (CPI), as per the below CPA mechanism.

Contract Price Adjustment will be applicable as from commencement of the 13th month of the contract period. Tenderers shall be entitled to claim contract price adjustment as follows:

90% of the tendered price will be subject to adjustment **annually** based on the **average** Consumer Price Index (CPI) as follows:

1st year:	12 months from date of commencement of contract. Firm – No request for price increases shall be entertained.
2nd year:	From start of 13th month to the end of the 24th month: Subject to contract price adjustment in accordance with the Consumer Price Index (P0141–Table B2 - CPI headline year-on-year rates). Base month for the price adjustment shall be three (3) calendar months prior to the date of commencement. The end month shall be three (3) calendar months prior to the 12th month.
3rd year:	From start of 25th month to end of the 36th month: Subject to the contract price adjustment in accordance with the Consumer Price Index (P0141–Table B2 - CPI headline year-on-year rates). Base month for the price adjustment shall be three (3) calendar months prior to the 13th month. The end month shall be three (3) calendar months prior to 24th month.
4th year:	From start of 37th month to end of the 48th month: Subject to the contract price adjustment in accordance with the Consumer Price Index (P0141–Table B2 - CPI headline year-on-year rates). Base month for the price adjustment shall be three (3) calendar months prior to the 25th month. The end month shall be three (3) calendar months prior to 36th month.
5th year:	From start of 49th month to end of the 60th month: Subject to the contract price adjustment in accordance with the Consumer Price Index (P0141–Table B2 - CPI headline year-on-year rates). Base month for the price adjustment shall be three (3) calendar months prior to the 37th month. The end month shall be three (3) calendar months prior to 48th month.
6th year:	From start of 61st month to end of the 72nd month: Subject to the contract price adjustment in accordance with the Consumer Price Index (P0141–Table B2 - CPI headline year-on-year rates). Base month for the price adjustment shall be three (3) calendar months prior to the 49th month. The end month shall be three (3) calendar months prior to 60th month.
7th year:	From start of 73rd month to end of the 84th month: Subject to the contract price adjustment in accordance with the Consumer Price Index (P0141–Table B2 - CPI headline year-on-year rates). Base month for the price adjustment shall be three (3) calendar months prior to the 61st month. The end month shall be three (3) calendar months prior to 72nd month.
8th year:	From start of 85th month to end of the 96th month: Subject to the contract price adjustment in accordance with the Consumer Price Index (P0141–Table B2 - CPI headline year-on-year rates). Base month for the price adjustment shall be three (3) calendar months prior to the 73rd month. The end month shall be three (3) calendar months prior to 84th month.
9th year:	From start of 97th month to end of the 108th month: Subject to the contract price adjustment in accordance with the Consumer Price Index (P0141–Table B2 - CPI headline year-on-year rates). Base month for the price adjustment shall be three (3) calendar months prior to the 85th month. The end month shall be three (3) calendar months prior to 96th month.
10th year:	From start of 109th month to end of the 120th month: Subject to the contract price adjustment in accordance with the Consumer Price Index (P0141–Table B2 - CPI headline year-on-year rates). Base month for the price adjustment shall be three (3) calendar months prior to the 97th month. The end month shall be three (3) calendar months prior to 108th month.

The **average CPI** calculated, the base month to the end month (both included) divided by the number
Of months.
The claim will be based on the **average** between the "base month" and the "end month" e.g.:
7+6+9+6 = 28 (28/4) = 7 therefore the claim will be 7%.

10% of the tendered rate will remain fixed.

8.3   CPA Process:

All requests for variation in the Contract price shall be submitted in writing as follows:
By email to: CPA.Request@capetown.gov.za and Siyanda.Mgudlwa@capetown.gov.za prior to the date upon
which the price adjustment would become effective.

8.3.1 When submitting a claim for contract price adjustment the Contractor shall indicate the actual amount
claimed for each item. A mere notification of a claim for contract price adjustment without stating the new price
claimed for each item shall, for the purpose of this clause, not be regarded as a valid claim. Contractor to apply
for contract price adjustment timeously.

8.3.2 The CCT reserves the right to withhold payment of any claim for contract price adjustment while only
provisional figures are available and until the final (revised) figures are issued by the relevant authority.

8.3.3 Process that will be followed:
- Contractor submits all the documentation indicated above prior to the effective date of the variation.

- The City will consider the variation and based on the documentary evidence, the City may approve the variation.

- Letters authorising the price variation will be communicated to the contractor indicating the effective date.

- All purchase orders for the contracted goods shall be issued at, and the Goods supplied, invoiced and paid for at the contract unit prices approved for that period and no further contract price adjustment claims will be considered, irrespective of the actual month of delivery and whether or not deliveries were subject to any manufacturing or delivery delays.

- All purchase orders from the effective date will be generated at the approved contract price. Purchase orders placed prior to the effective date will not be varied

Schedule 9: Certificate of Independent Tender Determination

I, the undersigned, in submitting this tender number **41S/2022/23 for the Supply, Installation, Service and Maintenance of a Records Management, Document Management and Case Management (RM&DM&CM) Solution for the City of Cape Town** in response to the tender invitation made by THE CITY OF CAPE TOWN, do hereby make the following statements, which I certify to be true and complete in every respect:

I certify, on behalf of :_____ (Name of tenderer)

That:

1. I have read and I understand the contents of this Certificate;
2. I understand that this tender will be disqualified if this Certificate is found not to be true and complete in every respect;
3. I am authorised by the tenderer to sign this Certificate, and to submit this tender, on behalf of the tenderer;
4. Each person whose signature appears on this tender has been authorised by the tenderer to determine the terms of, and to sign, the tender on behalf of the tenderer;
5. For the purposes of this Certificate and this tender, I understand that the word 'competitor' shall include any individual or organisation other than the tenderer, whether or not affiliated with the tenderer, who:
   (a) has been requested to submit a tender in response to this tender invitation;
   (b) could potentially submit a tender in response to this tender invitation, based on their qualifications, abilities or experience; and
   (c) provides the same goods and services as the tenderer and/or is in the same line of business as the tenderer.

6. The tenderer has arrived at this tender independently from and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium[1] will not be construed as collusive price quoting.

7. In particular, without limiting the generality of paragraphs 5 and 6 above, there has been no consultation, communication, agreement or arrangement with any competitor regarding:
   (a)   prices;
   (b)   geographical area where product or service will be rendered (market allocation);
   (c)   methods, factors or formulas used to calculate prices;
   (d)   the intention or decision to submit or not to submit a tender;
   (e)   the submission of a tender which does not meet the specifications and conditions of the tender; or
   (f)   tendering with the intention not to win the contract.

8. In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications and conditions or delivery particulars of the products or services to which this tender invitation relates.

9. The terms of this tender have not been and will not be disclosed by the tenderer, directly or indirectly, to any competitor, prior to the date and time of the official tender opening or of the awarding of the contract.

10. I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to tenders and contracts, tenders that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act, Act 89 of 1998, and/or may be reported to the National Prosecuting Authority (NPA) for criminal investigation, and/or may be restricted from conducting business with the public sector for a period not exceeding 10 (ten) years in terms of the Prevention and Combating of Corrupt Activities Act, Act 12 of 2004, or any other applicable legislation.

_____   _____
Signature   **Date**

_____
Name (PRINT)
(For and on behalf of the Tenderer (duly authorised))

(**[1] Consortium: Joint venture or Consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.**)

Schedule 10: Local Content Declaration / Annexure C

NOT APPLICABLE TO THIS TENDER

Schedule 12: Schedule of Pre-Qualification Criteria Sub-Contractors

NOT APPLICABLE TO THIS TENDER

Schedule 13: List of other documents attached by tenderer

	Date of Document	Title of Document or Description (refer to clauses / schedules of this tender document where applicable)
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		

Attach additional pages if more space is required.

_____   _____
Signature
Print name: Date
On behalf of the tenderer (duly authorised)

Schedule 14: Record of Addenda to Tender Documents

	Date	Title or Details
We confirm that the following communications received from the Employer before the submission of this tender offer, amending the tender documents, have been taken into account in this tender offer:		
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

Attach additional pages if more space is required.

SIGNED ON BEHALF OF TENDERER: . . . .

Schedule 15: Information to Be Provided With the Tender

Schedule 15A – Mandatory Requirement (Refer to paragraph 2.2.1.1.4 of the Eligibility Criteria)

Tenderers must be authorised or accredited by the OSM or copyright holder to sell or distribute the software solution and manage any warranty processes and escalations as and when required. Alternatively, should the authorization / accreditation be from a distributor, then a proof of authorization authorizing the distributor to resell and/or authorize others by the OSM or copyright holder, must be submitted.

Tenderers are to submit, either with their tender submission, or within a specified timeframe after being requested to do so; proof of authority from the OSM to sell/maintain/ support the products of the OSM or copyright holder.

SIGNED ON BEHALF OF TENDERER: . . . .

Schedule 15B – Evidence to Functionality Schedule: Experience of the Company providing RM&DM&CM Solutions (Refer paragraph 2.2.1.1.5.1 of the Eligibility Criteria)

Tenderer to demonstrate knowledge and experience in supply, implementation, transitioning, maintaining and supporting RM&DM&CM Solutions.

Please provide evidence of the number of continuous years the tenderer has been actively providing RM&DM&CM Solutions to their client base. This evidence must be in the form of reference letters, on the referee's letterhead, specifying the details and scope of the RM&DM&CM Solutions, the number of continuous years they have been actively receiving the RM&DM&CM Solutions from the tenderer, as well as all the referee's verifiable contact details.

CLIENT	SOLUTION PROVIDED	NUMBER OF YEARS (DATES/ DURATION)	REFERENCE – CONTACT NAME	REFERENCE – CONTACT EMAIL ADDRESS

SIGNED ON BEHALF OF TENDERER: . . . .

Schedule 15C – Evidence to Functionality Schedule: Size of organisation where a RM&DM&CM Solution has been implemented (Refer paragraph 2.2.1.1.5.2 of the Eligibility Criteria)

Tenderer to demonstrate the size of the organisation (Internal users) where a RM&DM&CM solution has been implemented at their clients indicating the number of users.

Please provide evidence in the form of verifiable references, specifying the number of internal and external users, as well as all the referee's verifiable contact details.

CLIENT	SOLUTION PROVIDED	NUMBER OF USERS (INTERNAL)	DATES/ DURATION	REFERENCE – NAME AND EMAIL ADDRESS

SIGNED ON BEHALF OF TENDERER: . . . .

Schedule 15D – Evidence to Functionality Schedule: Operational Experience Requirement (Refer to paragraph 2.2.1.1.5.3 of the Eligibility Criteria)

Tenderer to demonstrate experience in post implementation software maintenance and support of a RM&DM&CM solution for their clients.

Please provide evidence in the form of verifiable references, specifying the number of years providing operational maintenance and support, as well as all the referee's verifiable contact details.

CLIENT	DATES/ DURATION	REFERENCE – NAME AND EMAIL ADDRESS

SIGNED ON BEHALF OF TENDERER: . . . .

**Schedule 15E – Evidence to Functionality Schedule: Comparable Project / Client Requirement
(Refer to paragraph 2.2.1.1.5.4 of the Eligibility Criteria)**

Comparable Project / Client

Tenderer to demonstrate where a RM&DM&CM solution have been implemented within the last 5 years, with scope and clients comparable to the scope and requirements of the City of Cape Town

Please provide evidence, identifying the client indicating the size of the organisation in terms of number of system users, where a RM&DM&CM solution was implemented within the last 5 years, or where implementation is still in progress. This evidence must be in the form of reference letters, on the referee's letterhead with the referee's verifiable contact details to be included. Clearly identify if the client is a Public Sector client.

CLIENT	CLIENT SIZE	DATES/ DURATION	REFERENCE – NAME AND EMAIL ADDRESS

SIGNED ON BEHALF OF TENDERER: . . . .

Schedule 15F – Evidence to Functionality Schedule: Previous Implementation Project Value Requirement (Refer to paragraph 2.2.1.1.5.5 of the Eligibility Criteria)

Previous Implementation Project Value

Tenderer to demonstrate credibility with projects similar to the scope as required by the City in implementing, maintaining and supporting a RM&DM&CM Solution within the last 5 years. Refer to Section 13.1 in the specifications for the overview of the City's environment.

The tenderer must submit a list of successfully completed project(s) **within the last 5 years,** showing the value of the project, name of the client and verifiable contact details.

CLIENT	VALUE OF PROJECT	DATES/ DURATION	REFERENCE – NAME AND EMAIL ADDRESS

SIGNED ON BEHALF OF TENDERER: . . . .

Schedule 15G – Technical Schedule: Functional Requirements and Non-Functional Requirements for the RM&DM&CM Solution
(Refer to paragraph 2.2.1.1.6 of the Eligibility Criteria and paragraph 13.4.1 of Functional Requirements and 13.4.3 of Non-Functional Requirements)

The functional and non-functional requirements for the RM&DM&CM Solution are described below and tenderers must respond as indicated for each table.

These functional requirements definition is related to **SCHEDULE A** in section **(5) Price Schedule** of this tender document. The Tenderer must indicate in the column "**Compliant Yes / Partial /No**" whether the proposed solution adhere or can deliver on **ALL** the specified functional and non-functional requirements in each row. Where the proposed solution doesn't meet the requirements or partially meets the requirement, the Tenderer must clearly indicate which functional requirements cannot be delivered on and provide a response or explanation how this situation can be mitigated.

The Tenderer can also add relevant information as an annexure to the tender response with a clear reference to the item the information refers to. Please note clause **2.2.1 Eligibility Criteria** and **2.3.7. Test for responsiveness** on this matter.

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/Partial/ No)	Comment	On-Premises or Cloud
Records management, Case Management & Document Management The Content management system must allow for the integration of both physical record and document files, digital records, cases and documents to be organised so that they can be managed, found and understood.	It is implied that this incorporates: • Business classification scheme • Records and Document classification tools and • Folder Management • Case Management			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

Control
The Records Management Systems (RMS) must allow folders and records to be organised so that they can be managed, found and understood.
	Business classification scheme
	
	• The system should support the representation of a business classification scheme that reflects the business activity of an organisation.
	• Where the RMS supports a business classification scheme,
	
	   o it must be able to track the development and maintenance of the scheme over time and form part of the Enterprise Information Architecture.
	   o It must allow centralised management of the scheme by the RM System Administrator or other authorised user.
	   o it must allow the separate development and use of more than one scheme.
	   o it must allow the definition of levels and the allocation of unique identifiers for business functions, activities, and transactions.
	   o it should allow linkages between functions and activities to existing over time.
	   o it may allow the entry of text-based scope notes and other descriptive information attached to functions, activities, and transactions.
	   o it may allow the entry of start and end dates for functions, activities, and transactions.
	   o it may allow the entry of source citations or mandates attached to functions, activities, and transactions.
	   o it may allow the mapping of functions, activities, and transactions to organisational structures.
	   o it may allow links to one or more terms in			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	external schemes such as Keyword AAA: or the aka schema. o it may be able to import from, or export or link to, other systems where there is a close relationship between functional entities (as defined within the business classification scheme) and the functionality of other systems. o it may allow the entry or import of recordkeeping requirements for function/activity sets and transactions or groups of transactions. o it should enable links to records management mechanisms within the system – e.g. records classification tools, access controls and disposal classes/authorities. ▪ and the records management mechanisms within the system, it must warn a RM System Administrator when control mechanisms linked to the scheme are updated. ▪ and the records management mechanisms within the system, it must meet the metadata requirements specified for function entities as per the ISO international acceptable Record and Document management Metadata Standard			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	○ it should be able to export that scheme for use in a receiving system, maintaining all structural links between functions, activities, and transactions.			
	Records classification tools The RMS • must allow records to be classified in accordance with the organisation's records classification scheme. • must support close linkage and interaction between records classification tools and other record and document management processes such as capture, access and security, disposal, searching and retrieval, and reporting. • must support the definition of a records classification scheme, to organise digital folders and records. • must ensure that the hierarchical accumulation of RM&DM&CM within the definition of a records classification scheme, results in a unique record category. • must allocate a unique identifier to each term defined within a records classification scheme. • must allow a RM System Administrator or any other authorised user to make global amendments to the definition of a records classification scheme in a single process. • should not limit the number of levels permitted at different points within the definition of a records classification scheme. • must restrict the definition and maintenance of records classification tools to a RM System Administrator or any other authorised user.			
	Folder Management The RMS • must allow the addition of digital folders to the lowest levels of a defined records classification			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	scheme, to organise aggregations of digital records. • must be able to ensure that every folder is allocated to a record category within the records classification scheme. • should not limit the number of folders that can be allocated to a record category or defined within the entire system. • must allow a RM System Administrator to configure the naming mechanisms for entities within the record plan. • must be able to enforce the use of a records classification tool for naming new entities in the record plan. • must be able to automatically record the date of creation of a folder, as folder metadata. • must allow the separate entry of the date on which a folder was opened, which may precede the folder's date of creation. • must allow a folder or group of folders, and their attached records, to be moved and reclassified within the system by a RM System Administrator or any other authorised user. • must ensure that records attached to a folder remain correctly allocated following the reclassification of a folder so that all structural links remain in place. • must allow the manual or automatic update of all folder and record metadata attributes that are determined by classification, following the reclassification of a folder. • must allow a RM System Administrator or any other authorised user to enter (as folder metadata) the reason for the reclassification of a folder or group of folders in one operation. • must retain a history of folder reclassification, including a folder's original location. • must allow a RM System Administrator or any other authorised user to close a folder, ensuring that no new records can be added to that			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	folder (but noting the next requirement below). • must allow a RM System Administrator or any other authorised user to open a previously closed folder for the addition of records, and subsequently close the folder again. This will not automatically update the closure date retained in the folder metadata. The action is taken (i.e., the addition of records) must be recorded in the relevant audit trail. • must automatically record the closing date of a folder and be able to use this metadata to support other records management functions, such as disposal (see the disposal section). • must ensure that closed folders and their contents are still accessible for retrieval and viewing purposes. • must prevent the destruction or deletion of folders, records, and associated metadata at all times, except as specified in the Disposal section.			
	Records Metadata The RMS • must be able to capture and maintain metadata relating to any business classification scheme or records classification tools it supports, in accordance with the ISO Recordkeeping Metadata Standards and other relevant standards. • must prevent the unauthorised addition or amendment of metadata relating to a business classification scheme or records classification tools. • must enable lower levels in a defined records classification scheme hierarchy to inherit metadata from higher levels, at the time of creation. • should enable lower levels in a defined records classification scheme hierarchy to inherit metadata retrospectively, following a change to the metadata at a higher level.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	• must support the ability to amend or override inherited metadata by an authorised user. • must maintain a record of changes made to the business classification scheme or records classification tools over time. • must be able to capture and maintain folder metadata in accordance with the ISO Recordkeeping Metadata Standard for Commonwealth Agencies and other relevant standards. • The RMS must prevent the unauthorised addition or amendment of folder metadata elements. • must enable folders to inherit metadata from the records classification scheme at the time of the creation of the folders. • should enable folders to inherit metadata retrospectively, following a change to the records classification scheme. • must support the ability of an authorised user to amend or override metadata inherited by folders. • must allow user-defined metadata fields for the entry of descriptive information about the folder. • must closely link folder metadata to the functionality it represents. Folder metadata must provide both descriptive information and active support for achieving that functionality automatically.			
Capture *The system must formally capture records regardless of their technical characteristics.*	**Record capture** The RMS • must ensure that digital objects can be captured, regardless of format and technical characteristics, so that they can be registered and stored as digital records. • must allow users to capture, register and store all digital objects in their native format. • must be able to capture a digital object even if the generating application is not present. • must not limit the number of records that can be allocated to			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	a folder or captured within the entire system.
	• must be able to capture incoming and outgoing electronic messages and attachments:
	    ○ as an automated process; and/or
	    ○ as selected and directed by a user.
	• must be able to capture attachments and embedded objects together with electronic messages as either linked records or a single compound record.
	• must allow electronic messages and attachments to be captured from within an electronic messaging system, such as an email client.
	• must allow a user to choose whether to capture an electronic message, such as an email, with attachments as:
	    ○ an electronic message only;
	    ○ an electronic message with attachments;
	    ○ the attachments only;
	    ○ any combination of the above.
	• must be able to indicate whether an electronic message in the system has an attachment.
	• must be able to undertake the bulk capture of electronic messages relating to the same transaction.
	• must be able to capture a dynamic document, such as a dynamic web page, as:
	    ○ a single compound record;
	    ○ an aggregation of linked component records;
	    ○ a snapshot – 'frozen' in time;
	    ○ a collection of components that can be regenerated upon request; or
	    ○ a combination of the above
	• must support the capture of digital records from a range of records generating systems. These may include:			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	o common office packages;
	o workflow applications;
	o electronic messaging systems;
	o e-commerce and web transactions;
	o imaging and graphic design systems;
	o barcode support systems;
	o scanning applications
	o library management systems;
	o corporate systems;
	o business information systems;
	o security administration systems; and
	o multimedia applications.
	▪ must provide an application programming interface (API) to support integration with other business information systems, to enable the capture and processing of records of transactions in real-time.
	
	Bulk Record Imports
	The RMS
	• must be able to undertake a bulk import of records exported from other records management or document management systems, capturing:
	    o digital records in their existing format, maintaining their content and structure;
	    o digital records and their metadata, maintaining the relationships between them; and
	    o the folder structure to which the records are assigned and associated metadata maintaining the relationships between them.
	
	• must be able to perform a direct bulk import of digital records with associated metadata that is presented in accordance with the Record and Document Management Metadata Standard mapping this to the receiving structures.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	Record types The RMS ▪ must support the definition of different record types as defined by a RM System Administrator, ▪ must be able to manage record types centrally, (in a Centralised repository) restricting their use to groups of authorised users, ▪ allow defined record types to behave differently, according to their specified metadata profile and management policy and must support a default record type, which is available to all users with the ability to create records, provided within the system or as defined by the RM System Administrator.			
	Registration The RMS • must facilitate the registration process of records, in the case of a digital object, it must be marked as a formal record and registered into the corporate recordkeeping system. • must prevent any unauthorised amendment to the content of a registered digital record and must also always prevent the destruction or deletion of registered digital records and associated metadata, except as specified in the disposal section. Each registered record must have a viewable registry entry including associated metadata. • must be able to restrict the ability to amend the name of a registered digital record, • it must allow records and documents to be classified following the organisation's records and documents classification scheme at the time of registration. • must also prevent the storage of duplicate records. • shall provide a capability for referencing or linking and associating supporting and related records and related info such as notes, marginalia, attachments, and electronic			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	mail-return receipts, etc., to a specified record. • must allow only authorized individuals to change or delete links and associations. • must provide the capability to link original superseded records to their successor records. • shall provide the capability to support multiple renditions of a record. These shall be associated and linked. • shall provide the capability to increment versions of records when filing. The system shall associate and link the versions. • shall link the record metadata to the record so that it can be accessed for display, export, etc. • shall provide the capability for only authorized individuals to modify the metadata of stored records. However, the system shall not allow the editing of metadata fields that have been specifically identified in the regulations as not editable. • The system shall enforce data integrity, referential integrity, and relational integrity.			

	Filing Electronic Mail Messages (E-mail)
	The RMS
	• shall treat e-mail messages the same as any other record, and these shall be subject to all requirements of a record.
	• shall capture and automatically store the transmission and receipt data identified below if available from the e-mail system, as part of the record metadata when an e-mail message is filed as a record. The system shall provide the capability for editing
	
	    o Subject or Title,
	    o Author or Originator,
	    o Addressee(s), and
	    o the Other Addressee(s) metadata fields before filing. All other fields shall not be editable.
	• The Transmission and Receipt Data that must be capture includes:			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	o The intelligent name of the sender. The intelligent name refers to the birth name of the sender.
	    o The intelligent name of all primary addressees (or distribution lists).
	    o The intelligent name of all other addressees (or distribution lists).
	    o The date and time the message was sent.
	    o For messages received, the date and time the message was received (if available).
	    o The subject of the message.
	• The system shall provide the user with the option of filing e-mail and all its attachment(s) as a single record, or filing selected e-mail item(s) as an individual record(s), or to do both. When the attachment(s) is (are) filed as an individual record(s), the user shall be provided with the capability to enter the required metadata.			

	Record movement The RMS • must allow the re-assignment of records from one folder to another by a RM System Administrator or an authorised user and must be able to automatically capture metadata acquired directly from an authoring application, an operating system, or generated by the system itself. • must also capture electronic message transmission data such as e-mails and map it to record metadata elements. • must generate an alert when records are changed deleted moved copied etc.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
Access and security *The system must have the ability to assign rights and restrictions on the use or management of particular records to facilitate security and access control and integrate with the IS&T user access system*	**System access** The RMS • must allow for different roles to be created and assigned i.e. technical administration and business administration • must allow a RM System Administrator to set security parameters for failed login attempts and align these to the IS&T Directory Service Desk Authentication. • must provide a single sign-on screen that would provide access to the user for document management, record management, case management and GR documents based on the user access rights. • must support a mechanism for managing access and security controls centrally that may be applied to users, documents, cases and digital records and other entities in the record plan. The access control also refers to the deletion or making existing user access groups inactive, effectively barring any access previously allowed by the group(s) as per the CCT's access control policy.			
	User profile Management The RMS • must require a RM System Administrator to make users known to the system employing pre-defined user profiles, supporting valid authentication and the allocation of access and security controls, must allow (but not require) a RM System Administrator to allocate users to one or more pre-defined user access groups. • must ensure that all users are allocated one (or more) roles, and allow access only to system functions permitted by the role(s). based on the access and security controls linked to a role and inherited by users.			
	File plan • The RMS shall provide the capability for only authorized individuals to create, edit, and			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	delete file plan components and their identifiers. • The file plan components should be organized into logical sets that, when populated, will provide all the file plan references necessary to properly annotate (file) a record. • The system shall provide the capability for only authorized individuals to create, edit, and delete record folder components and their identifiers. Each component identifier shall be linked to its associated component and its higher-level file plan component identifier(s). • The system shall provide the capability to sort, view, save, and print user-selected portions of the file plan, including record folders.			
	Access and security metadata • The system must support the progressive addition of metadata to documents and digital records and folders to support access and security as per ISO standards for Record and Document Management Metadata. • The system should be able to retain the details and date of amendments to access and security controls, as historical metadata for a user profile, digital record, folder, or other record plan entity. • The system must support the progressive addition of metadata to documents and digital records and folders to support privacy, freedom and protection of information and archives legislation as and when these are published.			
	Access and security application The RMS must • allow each user to allocate to records and folders the same access and security controls contained in the user's profile.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	- prevent users from allocating access and security controls that are not contained in the user's profile. - support the allocation of all forms of access and security controls to digital records, folders and other record plan entities, including: - predefined user access groups (a discrete list of named users); - one or more individual usernames (an ad hoc list of named users); and - security categories (only one category may be allocated per entity)." - allow any and all combinations of access and security controls to be allocated to digital records, folders and other record plan entities. - allow the update and amendment of the access and security controls on digital records, folders, and other record plan entities. - restrict access to digital records, folders and other record plan entities that have been allocated a predefined user access group, to those users who are members of that group. - restrict access to digital records, folders and other record plan entities that have been allocated multiple predefined user access groups, to those users who are members of those groups. - limit access to digital records, folders and other record plan entities that have been allocated one or more individual usernames, only to those users so named. - allow all users (unless restricted by user role) access to all digital records, folders and other record plan entities which are not allocated any access or security controls. - restrict access to digital records, folders and other record plan entities, to those users or groups who have been allocated			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	an equivalent or higher security category. • ensure that digital records and folders automatically inherit access and security controls from higher levels of the record plan under which they are created. • allow inherited access and security controls to be overridden by an authorised user, in accordance with the organisation's security model. • be able to automatically upgrade the security category of a digital record or folder, in accordance with the organisation's security model. • require the allocation of a single security category to a digital record, folder or other record plan entity, with the default being the lowest category. • restrict access to digital records, folders and other record plan entities which have been allocated one or more forms of access and security controls, only to those users who have been allocated all equivalent controls – and prevent access by users who have been allocated some, but not all, equivalent controls.			
	Access and security metadata The RMS must • support the progressive addition of metadata to digital records and folders to support access and security as set out in the Record and Document Management Metadata standards • support the progressive addition of metadata to digital records and folders to support privacy, freedom of information and archives legislation, including: o information about the release of digital records and folders, which may be used to retrieve details from another system;			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	o disclosability and exemption indicators; and o full details of record creation, modification and preservation to assist in determining the age of long-term records,			
	Extraction • The system must allow the creation of an extract from a digital record, whereby sensitive information is removed or hidden from view in the extract, while the originating record remains intact, as well as provide solutions for expunging sensitive information from all record forms it can capture, including audio and video. • The system must note the creation of an extract in the metadata of the originating digital record, including date, time, creator and reason for the creation of the extract as well as be able to copy metadata attributes from the originating digital record to an extract – allowing selected elements to be amended as necessary.			
	Preserve records. The system should enable the organization to support the following capabilities in compliance with the records management policy(ies): • ensure that all records can be read and accurately interpreted throughout their useful life in that system; • enable migration of records to new storage media or formats to avoid loss due to media decay or technology obsolescence; • ensure that all captured metadata remains linked to appropriate records and is unchanged throughout the useful life of the records, including after migration to new media or technology; • monitor storage capacity and utilization, and alert system operators when action is needed			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	(e.g., to increase capacity, back-up system files).			

	Audit trail
	• The system must be able to automatically record information in the audit trail about the following events:
	  o creation of a new user or group;
	  o date and time of registration of all records;
	  o changes to access and security controls affecting a record, folder or user;
	  o relocation of records to another folder, identifying both origin and destination;
	  o relocation of a folder to a different part of the record plan, identifying both origin and destination;
	  o date and time of a change made to metadata associated with folders or records;
	  o all disposal review decisions made by a RM System Administrator;
	  o re-application of a disposal authority to an entity, identifying both previous and subsequent authorities.
	  o placing or removing a disposal freeze on a record or folder, and
	  o a separate log of all deletion or destruction actions carried out by any user.
	  o Create and maintain an audit trail (also called use-history metadata) for all records activity and system functions.
	  o Provide access to audit trail information in the fullest detail (e.g. each			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	individual record access, ○ including record identifier, time, date, and user). • Provide summary reports of audit trail information (e.g. number of accesses). • The track failed attempts of all records activity and system functions. • Maintain audit trail information (e.g., number of accesses, details of individual record retrievals, attempts to delete a record) so that it can be managed as a record.			
Disposal *The RMS must be able to control the retention and disposal of records held by the system, in accordance with disposal authorisation.*	**Disposal** • The system must be able to control the retention and disposal of objects held by the system (electronically or physically), in accordance with disposal authorisation regulations and guidelines whether WCARS or NARSSA. • The system should provide managed information storage and access as well as legal hold capabilities to ensure the preservation of information.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	Disposal authorities
	• The system must support the controlled disposal of records legally authorised for disposal, either following approved disposal authorities issued by the Western Cape (WC) Provincial Archives or under a specific legislative requirement for the disposal of particular records.
	• The system must support the definition and application of the following disposal actions:
	o review;
	o export;
	o transfer; and
	o destruction.
	• The system must be able to import and export a set of disposal classes in a standard format defined by the WC Provincial Archives.
	• The system must allow a unique identifier to be assigned to each disposal class and, where applicable, must allow the disposal class to be associated with the appropriate disposal authority.
	• The system must be able to maintain a history of all changes to disposal classes, including date of change and reason for change as well as restrict the ability to create, edit and delete disposal classes and disposal authorities to the RM System Administrator or other authorised user.
	• The system must ensure each disposal class consists of:
	   o a disposal trigger, to initiate the retention period;
	   o a retention period, to establish how long the record must be maintained; and
	   o a disposal action, to prescribe the fate of the record.
	• The system must allow retention periods to be defined from one day to an indefinite length of time and ensure that any amendments to a disposal class take immediate effect on all			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	objects to which that class has been applied.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	Disposal application
	• The system must allow disposal classes to be systematically applied to documents, digital records, folders and other record plan entities where supported.
	• The system must allow a disposal class to be applied at any level in the record plan, and inherited by descendant objects as they are created as well as enable the manual update or retrospective inheritance of disposal classes when a new disposal class is applied at a higher level of the record plan.
	• All disposal actions must be recorded in an audit trail
	• The system must support a disposal process consisting of:
	    o automatic identification of documents and digital records and folders for which the retention period has elapsed;
	    o execution of the relevant disposal actions after confirmation by a RM System Administrator or other authorised user.
	• Where the system supports folders, it must ensure that any disposal action applied at folder level is carried out on the complete folder contents.
	• The system must ensure that a retention period is calculated in real-time and cannot be artificially advanced and it must support external disposal triggers based on a notification of a defined event as entered by a user.
	• The system must automatically seek confirmation from a RM System Administrator or any other authorised user before implementing any disposal action and notify the RM System Administrator regularly of all disposal actions due to occur in a specified pre-defined period.
	• The system must allow a disposal freeze to be placed on a document, digital record, folder or other record plan entity, to prevent any disposal action			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	from taking place for the duration of the freeze and prevent the deletion of any object subject to a disposal freeze.
	• The system must be able to identify any conflict between disposal actions and either:
	    o automatically apply the correct disposal action according to precedence defined by the organisation; or
	    o notify the RM System Administrator or any other authorised user and request remedial action.
	• The system must generate a certificate for records which have been disposed			

	Scheduling Records. • The system shall provide the capability for only authorized individuals to view, create, edit, and delete disposition schedule components of record categories. • The system shall provide the capability for defining multiple phases (e.g., transfer to inactive on-site storage, transfer to off-site storage) within a disposition schedule. • The system shall provide the capability for only authorized individuals to define the cut-off criteria and, for each life cycle phase, the following disposition components for a record category: o Retention Period (e.g., fiscal year).			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	o Disposition Action (interim transfer, accession, permanent, or destroy).
	    o Interim Transfer or Accession Location (if applicable).
	• The system shall, as a minimum, be capable of scheduling and rescheduling each of the following three types of cut-off and disposition instructions:
	    o *Time Dispositions*, where records are eligible for disposition immediately after the conclusion of a fixed period of time following user-defined cut-off (e.g., days, months, years).
	    o *Event Dispositions*, where records are eligible for disposition immediately after a specified event takes place (i.e., the event acts as cut-off and there is no retention period).
	    o *Time-Event Dispositions*, where the timed retention periods are triggered after a specified event takes place (i.e., the event makes the record folder eligible for closing and/or cut-off and there is a retention period).
	• The system shall provide the capability to automatically calculate the complete life cycle, including intermediate phases, of record folders and records not in folders.
	• The system shall provide the capability for rescheduling dispositions of record folders and/or records (those not in folders) during any phase of their life cycle if an authorized individual changes the disposition instructions. This requirement includes the capability to change the cut-off criteria of disposition instructions and to change the retention			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	period associated with a disposition. • The system shall provide recalculation of the record life cycle based on changes to any life-cycle date and set the filing status (i.e., open, closed) of the folder according to the business rules associated with date change(s).			

	Review
	• The system must make all metadata relating to a digital record or folder under review available to the reviewer and must make the entire contents of a document or digital record or folder under review available to the reviewer, subject to applicable access restrictions. The applicable disposal class details must also be available to the reviewer either by searching or navigation.
	• When a review disposal action is triggered, the system must allow the RM System Administrator to reapply a disposal class which could:
	    o mark digital records and folders for further retention and later review;
	    o mark digital records and folders for immediate export, transfer, preservation treatment (through a technique such as migration) or destruction; or
	    o mark digital records and folders for further retention and later export, transfer, preservation treatment (through a technique such as migration) or destruction.			

	Export and transfer
	• The system must be able to export digital documents and records, folders or other record plan entities, and all associated metadata to:
	    o another system within the organisation;
	    o a system in a different organisation; or			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	o the Western Cape Provincial Archives for the long-term preservation of digital records or documents appraised as having archival value.
	• The system must ensure that any export action can include:
	  o all digital objects and folders that qualify for export under a disposal class;
	  o all metadata associated with exported digital objects, folders and other record plan entities; and
	  o all audit trail data associated with exported digital objects.
	• The system must be able to export groups of digital records or folders in one sequence of operations such that:
	  o the content and structure of digital records and folders are not degraded or corrupted.
	  o all components of a digital record or document are exported as one unit;
	  o associations are retained between exported objects and their metadata; and
	  o relationships are maintained between exported objects so that their structural links can be re-built in the receiving system.
	• The system must be able to export all the types of records it can capture, regardless of format or the presence of the generating application and must be able to export digital objects in their native format (or the current format to which they have been migrated).
	• The system must allow digital objects to be exported more than once and
	• must support a two-stage transfer process, consisting of:			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	o export of all digital records and folders that qualify for transfer under a disposal class; and o destruction of the exported digital records and folders following confirmation of successful export.			
	Destruction • The system must ensure that destruction results in the complete obliteration or inaccessibility of all objects as authorised, that they cannot be restored through operating system features or specialist data recovery techniques. • The system must prevent the destruction of digital records and documents or folders until a confirmation is received, and allow the process to be cancelled if confirmation is not received that will lead to all alternative renditions of that record are also destroyed. • The system must distinguish between an ad hoc delete function and the destruction function within the disposal process so that each can be allocated individually to authorised users. • The system must prevent the delete function from being used within the disposal process so that immediate destruction can only be achieved through the allocation of a disposal class.			
	Disposal metadata • The system must support the progressive addition of metadata to digital documents and records and folders to support disposal and must be able to export metadata in an XML format as set out in the Record and Document Management Metadata standards. • The system must be able to record the date and details of all disposal actions as a folder and/or record metadata.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
Searching and retrieval *The system must be able to retrieve digital records and folders by a variety of search methods, and render the results on-screen.*	**Search** • The system must provide search facilities to meet the needs of a range of users, from casual to sophisticated and must support the input of user-defined parameters to locate, access, retrieve and view records, folders and other record plan entities, and associated metadata. • The system must be able to withhold all or part of a search result, according to access and security controls as specified in the "Access and security" specification above. • The system must support the construction of searches by combining multiple terms from multiple sources. • The system must support the configuration of default search options for end-users as well as support the definition, saving and re-use of searches by end-users.			
	Retrieval • The system must be able to retrieve digital objects, documents or records and folders by all implemented naming principles as well as by their associated unique identifiers. • The system must be able to retrieve a complete folder and all its digital records and contextual metadata and list all and only those records in the context of that folder as a discrete group and a single retrieval process. • The system must be able to retrieve and list a set of digital objects, taken from many different folders, where the record metadata or content meets the search criteria, and it must also support the simultaneous retrieval of digital objects, folders and metadata by multiple users.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	• When the system is updated the URL link allocated to an artefact then the UTL or nickname must remain with the artefact to ensure that the document can easily be retrieved even in the future in a new location.			
	Display • The system must be able to display the content of all the types of digital records which it can capture, in a manner that presents all components of the digital document or record together as a unit in a manner that renders their original visual presentation and layout, without needing to load the generating application. • The system must be able to display all available metadata associated with a digital record or folder upon request. • The system should support the presentation or publication of digital objects, folders and associated metadata to a destination outside the system.			
	Printing • The system must be able to print all the types of digital objects it can capture, without the use of 'screen dumps' as it might be returned by a search query or all the digital records in a folder to be printed in one operation. • The system must enable the printing of metadata associated with digital records and folders, including the ability to print barcode labels. • The system must include features for the suitable output of digital records that cannot be printed.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
Metadata *The system must support the use of metadata to describe digital records, and to enable automated records processes.*	**Metadata configuration** • The system must support the range of metadata elements detailed in the Recordkeeping Metadata Standard as required by NARSSA and any other elements required to support the organisation's business and must be able to draw together all elements of metadata to create a metadata profile for a digital object, folder or other record plan entity where supported. • The system must place no practical limitation on the number of metadata elements allowed for each object in the system and must allow the RM System Administrator to specify which metadata elements are to be entered and maintained by keyboard entry or by drop-down list. • The system shall provide the capability for authorized individuals to designate the metadata fields that are to be constrained to selection lists and shall further provide the capability for authorized individuals to create and maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data. • The system shall provide the capability to allow only an authorized individual to define and attach user-defined business rules and/or access logic to any metadata field including user-defined fields.			
Compliance *The system must meet relevant local, national, and international requirements for record management*	**Legislation** • Consideration for the Protection of Personal Information Act promulgated in 2019 and effective in 2020, and the Promotion of Access to Information Act with input from City Legal as a stakeholder • The system must support compliance with the recordkeeping, evidential,			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	privacy and access provisions of all relevant South African legislation and regulations, including and not limited the to the following: o National Archives Act and Record Service of South Africa Act No 43 of 1996 (as amended Act No 36 of 2001); o Records Management Policy Manual National Archives and Records Service of South Africa, 2007; o National Records Management Policy. Records Management Policy Manual. National Archives and Records Service of South Africa, 2007; o Managing Electronic Records in Governmental Bodies: Policy, Principles and Requirements (2006); o Managing Electronic Records in Governmental Bodies: Metadata Requirements (2006); o Policy Framework for the Government-wide Monitoring and Evaluation Policy System 2007; o Minimum Information Security Standards of 1996 (MISS); o Minimum Interoperability Standards (MIOS) for Information Systems in Government; o Promotion of Administrative Justice Act (PAJA) 2000 (Act 3 of 2000); o Promotion of Access to Information Act (PAIA) 2000 (Act 2 of 2000);			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	o Protection of Personal Information Act (POPI) 2013 (Act 4 of 2013);
	   o Electronic Communications and Transactions Act (ECT) 2002 (Act 25 of 2002);
	   o Public Finance Management Act 1999 (Act 1 of 1999);
	   o Municipal Finance Management Act No. 56 of 2003 (MFMA);
	   o Law of Evidence Amendment Act 1988 (Act 45 of 1988);
	   o Companies Act;
	   o Financial Intelligence Centre Act;
	   o Financial Advisory and Intermediary Services Act;
	   o The Income Tax Act;
	   o VAT Act;
	   o Customs and Excise;
	   o Stamp Duties Act;
	   o Prescription Act;
	   o Insolvency Act;
	   o King IV Code.			

	Standards • Updates to ISO/DIS/SANS 16175: Information and documentation - Processes and functional requirements for software for managing records and to Relationship between the ISO/SANS 16175 series of standards and other products of ISO/TC46/SCII: Archives/Records Management • The system should support compliance with all applicable South African and international standards. The standards do not replace the requirements contained in the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) (NARSSA Act) but affirm and support the statutory requirements. • NARSSA endorses the standards listed below in so far as they serve as benchmarking			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	tools for sound records management in governmental bodies and guide governmental bodies regarding other archival matters.
	• Some, and not all, of the applicable standards are listed below:
	   ◦ ISO (SANS) 15489:2016 – Information and documentation – Records Management Part 1 and 2;
	   ◦ ISO (SANS) 15801:2017 – Document management - Information stored electronically - Recommendations for trustworthiness and reliability;
	   ◦ ISO (SANS) 30300:2020 – Information and documentation – Records Management – Core Concepts and Vocabulary;
	   ◦ ISO (SANS) 30301:2011 – Information and documentation – Management Systems for Records – Requirements;
	   ◦ ISO (SANS) 30302:2015 – Information and documentation – Management Systems for Records – Guidelines for Implementation;
	   ◦ ISO (SANS) 23081-1:2017 - Information and documentation - Records management processes - Metadata for records Part 1: Principles;
	   ◦ ISO (SANS) 23081-2:2009 - Information and documentation –			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	Managing metadata for records Part 2: Conceptual and implementation issues; ○ ISO (SANS) 1828:2014 – Information and Documentation – Risk Assessment for Records Processes and Systems; ○ ISO (SANS) 18492:2005 Long-term Preservation of Electronic Document-Based Information; ○ ISO (SANS) 17799:2005 – Information Technology Security techniques – code of practice for information security management; ○ ISO (SANS) 14721:2012 – The Open Archival Information System (OAIS) Reference Model: Introductory Guide; ○ ISO (SANS)19005-1:2005 - Document management - Electronic document file format for long-term preservation Part 1: Use of PDF 1.4 (PDF/A-1); ○ SANS 19005-2:2011 - Document management - Electronic document file format for long-term preservation Part 2: Use of ISO 32000-1 (PDF/A-2); ○ SANS 16175-1:2014 - Information and documentation - Principles and functional requirements for records in electronic office environments - Part 1: Overview and statement of principles (Based on ICA-Req Module 1);			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud

	o SANS 16175-2:2014 - Information and documentation - Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems (Based on ICA-Req Module 2);
	   o ISO (SANS) 16175-3:2014 - Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 3: Guidelines and functional requirements for records in business systems (Based on ICA-Req Module 3);
	   o ISO/TR (SANS) 13028:2010 - Information and documentation - Implementation guidelines for the digitization of records;
	   o ISO (SANS) 25964:2011 - Thesauri and interoperability with other vocabularies – Part 1 Thesauri for information retrieval;
	   o ISO (SANS) 25964:2013 - Thesauri and interoperability with other vocabularies – Part 2 Interoperability with other vocabularies.			

	Guidelines • Consideration should also be given to the CCT's policies as well as the policies and protocols as specified by the Western Cape Government's WCARS (Western Cape Archives and Records Service). • The system should support best practice following all applicable			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comment	On-Premise or Cloud
	NARRSA guidelines, including all other relevant guidelines where relevant. • The list below contains some of the guidelines that the system needs to adhere too and enforce: o The DOD 5015.2-Standard; o CCT Records Management System and Procedure; o CCT Information Security SOP; o CCT Electronic Communication SOP; o CCT Electronic Mail Usage Rules; o CCT IT Continuity SOP o CCT Business Continuity SOP; o CCT Data Strategy; o WCARS Digital Preservation Policy; o WCARS Naming Convention Protocol; o WCARS Digitalization Policy.			
Storing Records The RMS must store records in a repository and these records must be accessed and managed through integration	• The system shall provide at least one portal that provides access to all associated repositories and databases storing electronic records and their metadata. • The system shall prevent unauthorized access to the repository (ies). • The system shall manage and preserve any record in any supported repository, regardless of its format or structure, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original. • The system shall allow only authorized individuals to move or delete records from the repository.			

Document Management - Functional Requirement Category-	Document Management - Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
Document management *The Electronic Document Management System (EDMS) must be able to provide, or integrate with, document management facilities to ensure records management functions are seamlessly supported.*	**Control** • The system with document management facilities must make a clear and obvious distinction between digital documents and registered digital records. • The system must provide options for registering all unregistered digital documents in a particular folder or folders as formal records, in a single process. • The system must allow automatic deletion of all unregistered digital documents in a particular folder in one process, or after a set period.			

	Capture
	The system with document management facilities must be able to:
	• capture and register in one process:
	   o a newly created digital document; and
	   o a digital document already existing in the document management environment.
	• capture a digital document and allow the option of completing the registration process at a later time.
	• allow users to transfer smoothly between the document management environment and the system to register a digital document as a record.
	• Automatically create versions of digital documents, without automatically creating a new digital record.
	• copy a digital record to make a new digital document, ensuring the digital record remains unaffected.
	• manage versions in a tightly bound relationship, to support drafting and ensure the integrity of the digital document as a whole.
	• provide options for registering some or all versions of a digital document as digital records.			

	Access and security • The system with document management facilities must not allow ownership rights from the document management environment to apply to a registered digital record. • The system with document management facilities must not allow a registered digital record to be checked out, where this would allow the alteration of record content in any way.			
	Disposal • The system with document management facilities must be able to detect digital documents in any folder due for export or transfer and notify the RM System Administrator. • The system with document management facilities must enable digital documents to be registered as records before export or transfer. • The system with document management facilities must be able to export only registered digital records. • The system with document management facilities must automatically destroy digital documents when the digital records to which those documents relate are destroyed after a successful transfer process.			

	Searching and retrieval
	• The system with document management facilities should have the ability to retrieve documents along with records, using the same search interface.
	• The system should allow an authorised user to configure the retrieval of documents to:
	  o the latest version only;
	  o selected versions only;
	  o only those versions registered as records; or
	  o all versions of the document.			

	Metadata • The system with document management facilities must support the mapping of digital document metadata to digital record metadata, as set out in the Record and Document Metadata Standards.			

	• The system with document management facilities must support the definition of templates for common digital documents, and the allocation of different metadata set for each template. • The system with document management facilities must ensure that any metadata captured in the document management environment is managed under the requirements of the system specifications, to ensure its authenticity. • The system with document management facilities must allow metadata to be captured from a user at the time of capture and registration.			
Conversion to a Record	**Converting a Document to a Record** • The system should allow the user to right-click on the document once selected and then select the option to convert the document to a record or the system should provide a similar icon-driven event to trigger the conversion. • All related metadata and taxonomy information must be carried forward with the document in the creation of the record			

Compliance
The system must meet relevant local, national, and international requirements for document management
	Legislation
	• Consideration for the Protection of Personal Information Act promulgated in 2019 and effective in 2020, and the Promotion of Access to Information Act with input from City Legal as a stakeholder
	• The system must support compliance with the document management, evidential, privacy and access provisions of all relevant South African legislation and regulations, including and not limited the to the following:
	    o Policy Framework for the Government-wide Monitoring and Evaluation Policy System 2007;
	    o Minimum Information Security Standards of 1996 (MISS);
	    o Minimum Interoperability Standards (MIOS) for Information Systems in Government;
	    o Promotion of Administrative Justice Act			

	(PAJA) 2000 (Act 3 of 2000);
	   ○ Promotion of Access to Information Act (PAIA) 2000 (Act 2 of 2000);
	   ○ Protection of Personal Information Act (POPI) 2013 (Act 4 of 2013);
	   ○ Electronic Communications and Transactions Act (ECT) 2002 (Act 25 of 2002);
	   ○ Public Finance Management Act 1999 (Act 1 of 1999);
	   ○ Municipal Finance Management Act No. 56 of 2003 (MFMA);
	   ○ Law of Evidence Amendment Act 1988 (Act 45 of 1988);
	   ○ Companies Act;
	   ○ Financial Intelligence Centre Act;
	   ○ Financial Advisory and Intermediary Services Act;
	   ○ The Income Tax Act;
	   ○ VAT Act;
	   ○ Customs and Excise;
	   ○ Stamp Duties Act;
	   ○ Prescription Act;
	   ○ Insolvency Act;
	   ○ King IV Code.			

	Standards • Updates to ISO/DIS/SANS 16175: Information and documentation - Processes and functional requirements for software for managing records and to Relationship between the ISO/SANS 16175 series of standards and other products of ISO/TC46/SCII: Archives/Records Management • The system should support compliance with all applicable South African and international standards. The standards do not replace the requirements contained in the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) (NARSSA Act) but affirm and support the statutory requirements. • Some, and not all, of the applicable standards applicable to			

	document management are listed below: o ISO (SANS) 15801:2017 – Document management - Information stored electronically - Recommendations for trustworthiness and reliability; o ISO (SANS) 18492:2005 Long-term Preservation of Electronic Document-Based Information; o ISO (SANS) 17799:2005 – Information Technology Security techniques – code of practice for information security management; o ISO (SANS) 14721:2012 – The Open Archival Information System (OAIS) Reference Model: Introductory Guide; o ISO (SANS)19005-1:2005 - Document management - Electronic document file format for long-term preservation Part 1: Use of PDF 1.4 (PDF/A-1); o SANS 19005-2:2011 - Document management - Electronic document file format for long-term preservation Part 2: Use of ISO 32000-1 (PDF/A-2); o ISO (SANS) 25964:2011 - Thesauri and interoperability with other vocabularies – Part 1 Thesauri for information retrieval; o ISO (SANS) 25964:2013 - Thesauri and interoperability with other vocabularies – Part 2 Interoperability with other vocabularies.			
	Guidelines • Consideration should also be given to the CCT's policies as well as the policies and protocols as specified by the Western Cape Government's WCARS (Western Cape Archives and Records Service).			

	• The list below contains some of the guidelines that the system needs to adhere too and enforce:
	    o The DOD 5015.2-Standard;
	    o CCT Records Management System and Procedure;
	    o CCT Information Security SOP;
	    o CCT Electronic Communication SOP;
	    o CCT Electronic Mail Usage Rules;
	    o CCT IT Continuity SOP
	    o CCT Business Continuity SOP;
	    o CCT Data Strategy;
	    o WCARS Digital Preservation Policy;
	    o WCARS Naming Convention Protocol;
	    o WCARS Digitalization Policy.			

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
Usability *The RM&DM&CM system must be logical to operate and simple to learn, taking into account the differing needs and abilities of potential users.*	**User interfaces** • The system must provide a user interface that complies with the accepted standard rules for the operating system or platform on which it will operate and where it supports a web browser interface, it must meet internationally accepted guidelines for web design. • The system user interface must be presented consistently across all windows, menus, commands and other facilities and need to provide a single sign-in and access to the objects, documents, records and case management modules.			
	Usability of system functions • The system must produce meaningful error messages that offer a simple method of correcting the error or cancelling the process supported by an online context-sensitive help facility, including help on the use of the records classification scheme where supported as well as a spell-check facility at all data-entry stages, including searching. • The system must ensure that minimal movement between screens is required to perform system operations and must make consistent use of function keys, hot-keys and short-cut keys across all components of the system. • The system must be able to hide system functions from users who do not have permission to use them and also prevent users from carrying out the initial steps of a process they will be unable to complete due to functional permission restrictions. • The system must ensure that its facilities are as intuitive and			

<table>
<tr>
<td></td>
<td>easy to use as possible by allowing:
    o functions to be performed with as few mouse clicks or keystrokes as possible; and
    o the completion of routine functions from one screen.

• To allow records to be captured by the system with minimal user intervention, the system must be capable of integrating or interfacing with (as required):
    o standard office suite applications;
    o standard electronic messaging systems, such as email, SMS and WhatsApp (or any other social messaging system) clients;
    o other mainstream applications already installed, and particular business information systems used by the organisation.

• The system must be able to generate an electronic message from within the system, to attach:
    o digital records and documents;
    o metadata; and/or
    o active pointers to records and/or metadata.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>**Reporting**
The system must be able to produce reports on system activities and the status of objects within its control, for management, statistical and general purposes.</td>
<td>**Report management**
• The system must provide a reporting capability to produce management, statistical and ad hoc reports on system activity based on restriction on end-user's access to selected reports, or the reporting function in general.
• The system must allow reports generated to be saved, modified and re-used in the future and it must also allow reports generated to be easily exported from the system using one or more common data formats (such as plain text,</td>
<td></td>
<td></td>
<td></td>
</tr>
</table>

	comma-separated value, or tab-delimited computer file types).
	• The system should be able to export the information in JSON and XML standards or any industry-accepted standard in the future.

	Reporting on classification tools
	• Where the system supports a records classification scheme or business classification scheme, it must be able to generate a report comprising: 　○ the entire scheme; and 　○ a part of the scheme (e.g., a specified function and its related activity RM&DM&CM), indicating the relationship between RM&DM&CM in a hierarchical format.

	Reporting on folders and records
	• The system must be able to produce reports listing: 　○ all folders classified within the records classifications scheme; and 　○ all folders classified in a section of the records classification scheme, structured according to the hierarchy of the record plan or other classification tool. • The system must be able to produce statistics for the number and location of: 　○ digital records by application type and version; and 　○ digital records and folders by specific access and security controls. • The system must be able to produce a report listing the details and outcome of any migration process, to ensure the integrity of digital records. • The system must be able to report on the size and

	remaining capacity of its digital record stores and repositories.			

	Reporting on user activity
	• The system must be able to report the actions carried out by a particular user, or group of users, during a specified date range.
	• The system must be able to generate a list of all, or a subset of, user profiles known to the system.
	• The system must be able to produce statistics for the number of records
	    ○ and folders created by a user or group of users for a defined period; and
	    ○ viewed by a user or group of users within a defined period.			

	Reporting on access and security
	• The system must be able to report all attempts at unauthorised access to the RM System Administrator.
	• The system must be able to
	    ○ generate a report based on selected access controls and security controls.
	    ○ report on all alterations to access permissions, access controls and security controls, within a specified period.
	    ○ to generate a list of all, or a subset of, user access groups known to the system.			

	Reporting on disposal activity
	• The system must be able to produce reports on all disposal activity undertaken by the system.
	• The system must be able to produce a report listing:
	    ○ all disposal classes currently defined in the system;
	    ○ all digital records, folders or other record plan entities (where supported) to which a			

	particular disposal class is currently applied;
	   o all objects for which a particular disposal action will occur, over a given period; and
	   o all objects due for disposal within a given period
	• The system must be able to report on all objects subject to a disposal freeze.
	• The system must be able to produce:
	   o statistics of review decisions over a given period;
	   o a report detailing any failure during export of objects from the system, identifying objects that have generated processing errors or were not successfully exported;
	   o a report detailing the outcome of a destruction process, detailing all objects successfully destroyed and identifying those objects which that were not successfully destroyed; and
	   o report on the volume and types of objects that are overdue for disposal.			

System administration The system must provide facilities for the ongoing maintenance and support of the system, and the data it manages. Some of these functions may be provided by the operating system, database management system or other applications linked to the system. Clearly indicate if the	**Data processes** • The system must automatically invoke checks that system operations are successfully performed on transactional data. • The system must support automatic data validation rules. **Deletion of records** (For information on records destruction, see the Disposal section) • The system must allow a default or option that prevents any user or RM System Administrator from changing, moving or deleting in an ad hoc manner a digital record or object once captured.			

| system provides the functionality or if it relies on other third-party capabilities to provide these functionalities | • The system must ensure that any function to delete digital records or folders on an ad hoc basis (outside the disposal process) is restricted to the very highest level of RM System Administrator.
• Where the system allows deletion of a digital record, folder or other record plan entity, it must:
 o ensure that no objects are deleted if their deletion would result in a change to another object;
 o notify the RM System Administrator of any objects linked to the object about to be deleted;
 o seek confirmation from an authorised user before proceeding with deletion;
 o delete the entire contents of the object;
 o record the deletion comprehensively in the audit trail; and
 o produce an exception report.
• The system must support the retention of metadata for digital records, folders and other record plan entities that have been deleted.
• The system must allow a RM System Administrator to amend user-entered metadata, as part of an audited procedure.
• The system must prevent the deletion of metadata that is associated with an object under the control of the system. | | | |
| | **Storage**
• Subject to the metadata requirements, the system must support the storage of digital records and associated metadata either:
 o together in a digital repository that is an integrated part of the system; or
 o separately, with records maintained in the native | | | |

	software environment, and metadata under the control of a system.			
	• The system must provide facilities for monitoring digital repositories and must warn a RM System Administrator when storage limits are about to be reached.			
	• The system must be able to prevent or resolve any conflicts caused by changes to storage locations.			
	• The system must support automated back-up and recovery facilities for all (or selected) entities, metadata, audit trails and configuration settings held by the system based on the manual configuration of the frequency of back-ups, and elements of the system to be backed up.			

	• The system must allow a RM System Administrator to restore the entire system
	    o from backups, maintaining full data integrity to ensure business continuity;
	    o from the most recent back-up to the point of system failure.			

	• The system must provide notification of any data updates that were unable to be recovered or rebuilt.			
	• The system must support the identification of vital records that are critical to business continuity.			
	• The system shall provide the capability to automatically synchronize multiple databases and repositories.			
	Preservation • The system must be able to manage digital objects according to the minimum mandatory requirement of this document over time, to ensure their integrity and support long-term preservation.			
	• The system must support automatic and manual mapping to and from the system metadata fields.			

	• The system developer must have a routine in place to ensure that digital records remain accessible and retain their integrity after a system upgrade. • The system must use and house all storage media in environments that are compatible with expected life, and within a tolerance of the media manufacturer's specification. • The system must ensure that all tailored modifications are brought forward and are operational when system upgrades are implemented without the need to recreate and redevelop these customisations again. • The system must be able to migrate digital records, folders, physical registry files and other record plan entities (where supported) following the requirements for export and bulk import listed in the section above. • The system must be able to perform bulk conversion of digital records to other media and/or systems in line with the standards relevant to their format(s), for example, PDF/A for long term preservation and PDF/J for architectural documents. • The system must ensure that no data is lost or corrupted during system upgrades, migration or conversion. • The system must support periodic refreshing of storage media, to guard against media degradation.			
System design *The system design must support response times and levels of system availability that meet current and projected user requirements.*	**Performance** • The system must provide a stable and flexible architecture that can grow to meet changing business needs, and continue to meet the recordkeeping requirements appropriate to its particular implementation. • The system must be able to consistently perform all functions to a specified standard which meets business needs and user expectations. (see the non-			

	functional requirements for some parameters).
	• The system must demonstrate acceptable response times for commonly performed functions, under normal operating conditions. Benchmark measures for performance may include the time taken to:
	    o display a graphical view of the record plan;
	    o store standard documents at capture and/or registration;
	    o return a search response for a simple query;
	    o return a search response for a complex query; and
	    o display text missing.
	
	The system must provide:
	• Centralized back-up and restore
	• GUI administration accessible to Administrator
	• Out-of-the-box Load management
	• Supports Network Load Balancing and Clustering
	• High throughput and scalability			

	Scalability
	• The system must be capable of controlled growth, to continue to meet anticipated organisational needs over time.
	• The system must demonstrate its capacity to handle the projected needs of the organisation, whilst maintaining the expected performance measurements stated previously. Indicators of scalability may include whether:
	    o the maximum size of the digital repository will be able to accommodate the expected total number of records;
	    o the number of geographical locations across which text to complete which the system will meet anticipated organisational needs;
	    o the total number of users that can be supported will accommodate predicted staff increases;			

	o the amount of systems administration and re-configuration down-time required to support projected numbers of records and users during the first five years of operation falls within acceptable parameters; and o the amount of downtime required to make bulk changes to organisational structures, classification tools and user roles (with the number of folders, records and users anticipated after five years of operation) will fall within specified acceptable parameters.				

	Reliability and control
	• The system must demonstrate its capacity to remain available and operational, as required to meet business needs. Measures for reliability may include:
	    o specified hours of the day, or days of the year, during which the system must be available;
	    o range of planned or unplanned downtime that can be tolerated; and
	    o the acceptable period required to restore the system from back-up in the event of system failure.
	• The system must have the ability to enforce data integrity, referential integrity and relational integrity at all times.
	• The system must ensure that all entities (e.g., folders, records, extracts) are allocated a unique system identifier.				

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement	COMPLY (YES/No)	Comments	On-Premise or Cloud
CASE MANAGEMENT *Refers to an application designed to support a complex process that requires a combination of human tasks and electronic workflow- enabled through workflow, management collaboration, storage of images and content, decisions, and processing of electronic files or cases*	**Workflow Engine** The system must have a workflow engine to support different types of document routing mechanism including: o Sequential routing - Tasks are to be performed one after the other in a sequence. o Parallel routing - Tasks are split among multiple users and then merged as a single composite work item through the support of conditional merging of the multiple parallel activities. o Rule-based routing - One or another task is to be performed, depending on predefined rules. o Ad-hoc routing - Changing the routing sequence by authorized staff with the appropriate access and rights. The system should support the registering and configuring of third-party applications.			
	Process Design • The system must have a built-in Graphics based workflow designer to design Business Processes based on BPMN ver2.1 standard. Any process design or modification should be performed without the need for programming expertise, • The Process designer must have an intuitive interface to assist in the design of complex rules and conditions for workflow routing. • The system shall allow the creation and the storage of sub-processes and allow the re-use of the sub-processes across the Enterprise to enable uniformity in process actions and the enablement of agility.			

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement	COMPLY (YES/No)	Comments	On-Premise or Cloud
	• The system should provide a facility to define multiple archive stages to archive selected documents and indexes in the underlying Document management system at any stage of the workflow process. • The system must provide the capability to define hold stages so that a particular instance of the workflow can be kept on hold for specified interval based on the pre-defined condition as well as the facility to define the conditions for resuming the instance that is in the hold stage. • The workflow management system shall support the definition of roles and allow many-to-many relationships between users and roles to be defined. • The system must provide the facility to assign ad hoc tasks at runtime to users.			
	Form Designer • The system must provide a built-in facility to design custom forms that can be attached at one or more stages in the workflow. • The Form designer interface shall enable the user to define text boxes, Combo boxes, radio buttons, Dropdown etc. • The system shall support field-level calculations at form level as well as scripts to control field level validations. • The system shall provide a facility to define variables in the process or in external database tables, which can be linked to fields defined in the form for efficient data entry.			
	Exceptions Handling • The system must enable the CCT to define exceptions per stage if required, which shall dynamically alter the process flow on execution.			

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement	COMPLY (YES/No)	Comments	On-Premise or Cloud
	• The RM Administrator shall have the ability to grant rights to raise and clear exceptions at different stages of the process annotated with user comments. • The system must be able to raise triggers based on exceptions. • The system should provide a facility to raise automatic exceptions based on pre-defined conditions. • The system shall track all the exceptions raised in the course of the process and shall maintain the history of that with the user's name, date, time and comments. • The system must be able to differentiate process instances with and without exception • The system must have a built-in Rule Engine that will be used for defining business and process rules.			
	Triggers Handling • The system must allow the authorised users to define custom triggers like Emails, Word template or launching executables on predefined conditions. • The system must have a facility to define custom trigger templates that can utilise static and dynamic data. • The system must have the ability to generate event-based triggers that will automatically send emails/ fax, generate responses, invoking data forms to capture data as well as invoking communications with external systems. • The workflow management system must send an email notification to a user when the user is not logged into the workflow management system. If the user on the URL in the email, then the system must automatically			

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement	COMPLY (YES/No)	Comments	On-Premise or Cloud
	launch the Workflow management system and present the user with the task to perform.			

	Process Monitoring and Reporting
	• The workflow management system must track and be able to display in graphical and in tabular format the worktime status, the date/time the task started and ended as well as the creation and archival date of the documents.
	• The system must provide the users with the ability to configure without requiring any coding the dashboard for specific roles e.g., dashboard for a director, a dashboard for Administrator, etc.
	• There should not be any limit on the number of reports that can be created in the system.
	• The User must be able to drill down into a report for specific information analysis.
	• The workflow management system shall support the generation of statistical and management reports like:
	    o Average Process Time Report
	    o Diversion Report
	    o Exception Details Report
	    o Expired Work-item Report
	    o Number of pending files
	    o Participant Processing Time Report
	    o Participant Report
	    o Process Definition Summary Report
	    o Process History Report
	    o Time is taken to complete each task
	    o User Performance Report			

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement	COMPLY (YES/No)	Comments	On-Premise or Cloud
	o Performance comparison reports. o Total turnaround time and o Delay report for complete process or specific work stages • The system must incorporate an administration module to configure the user, groups, queue related to a process. It is recommended that these setting must be captured in the central RM&DM&CM configuration tables.			
	User Management and Security • The workflow management system shall support integration with Lightweight Directory Access Protocol (LDAP) for domain-level authentication and single sign-on or whichever future Access management protocol that the CCT will use. • The workflow management system shall support integration with database authentication as per the CCT's protocols. • The workflow management system shall be capable of giving access rights to users/groups on work stages, documents, forms and data fields. • The workflow management system shall support extensive password validations i.e. locking of a user account after the specified number of unsuccessful login attempts, password history, password expiry, passwords must be alphanumeric and of minimum character length etc. • The workflow management system shall support SSL, HTTPS and any other session timeouts that might be required by the CCT.			

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement	COMPLY (YES/No)	Comments	On-Premise or Cloud
	Administration and System Management • System and Business administration access rights need to be different to ensure users are managed by the business and the system variables by the RM System Administrator.			

	Business rules management
	• The system should support a business analyst to define business rules, associate the rules with business processes and business rules management.
	• The platform must come with tools that allow business rules to be easily authored by business users without any technical help from IT.
	• The system must have the ability to expose rules as APIs/Web service to be consumed by 3rd party applications.
	• The system must also provide the following functions:
	    o Rule versioning management
	    o Web-Based User Interface for Business Users to Edit Rules
	    o Manage an unlimited number of rules.
	• The system must have a master data management (MDM) module where all process-related master tables can be defined via a user-friendly GUI interface.			

	Audit Trails
	The system should support capturing of an audit trail for the following but not limited:
	    o Workflow events
	    o User assignments/releases
	    o Notifications			

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature	Comply (Yes/No)	Comments	On-Premise or Cloud
Onboarding and Registering *Onboarding is the process of registering new and existing customers, ensuring that they access all the services and products contracted in a simple and fast way, integrating into the company's customer base. This forms part of the 3-way authentication required in some digital signatures.*	The system should allow for proactive onboarding of signatories as per the customer's/signatory's subscriber agreements. • Ability to on-board a signatory before documents needing to be signed. i.e., proactively onboarding customers/signatories, as soon as the subscriber agreement is signed, to ensure a seamless process when signing.			
	The system is to allow customers/signatories to register on the signing platform with appropriate login credentials which they can use going forward. This includes the customer agreeing to the terms of the Advanced Electronic Subscriber Agreement (AESA). • New customers/signatories should be able to register a profile with the necessary details (ID number, name, surname, email address, cell phone number, etc.). • Security questions are also to be included as part of the registration process. • Advanced Electronic Subscriber Agreement (AESA) - Once signed, the digital copy is to be automatically uploaded to Record Management System under the correct taxonomy.			
Signatures – including multiple signatures	The system should allow for multiple signatories to sign a document/s. • Email notifications informing signatories that their documents are ready to be signed should be sent in the order that the signatories were captured. • Only once the first signatory has signed all documentation in the pack, should the next signatory get a notification that they can commence with the signing process and so forth (for the remaining signatories).			

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature	Comply (Yes/No)	Comments	On-Premise or Cloud
	• The system should only upload the document sets that pertain to the electronic method of signing. • The system should have the ability when drafting the contract to identify whether the client is signing electronically or face-to-face to ensure that the document set has witness requirements or not according to the customer's/entity's signing method/preference indication. • The different versions of the contract document should be saved in the Document Management System with version control and the required metadata • Once the final signature is received, then the contract record must be saved to the Records Management system and logged to make the document immutable.			
	Once a document has been signed, the system should have the ability to apply the customer's/signatory's initial on each page in the document that was signed, • Once the customer/signatory has signed the document, the system must automatically apply their initials on each page within that document			
	The system should allow signatories to view all past signed contracts. • Signatories must always be able to log back into the system and view all previously signed contracts or use the RMS to view these records			
Customer communication	The system must send an email and/or SMS to the customer informing them that their documentation has been drafted and is ready to sign.' • Communication must notify the customer/signatories to access the platform. • In the case of multiple signatories, the same communication is to be sent to all relevant parties.			

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature	Comply (Yes/No)	Comments	On-Premise or Cloud
Use of One-Time-Pin (OTP)	The system must make use of a one-time pin (OTP) sent to the customer/signatory for accessing the platform. • The customer/signatory should be able to choose if they would like the one-time pin (OTP) sent to their cell phone number or email address. • If the customer/signatory is a new user, the OTP should be sent to the cell phone number or email address that the customer captures as part of the registration process. • If the customer/signatory is an existing registered user, the OTP should be sent to the cell phone number or email address on record for that customer.			
	The system should allow for signatories to sign documents separately (one at a time) and all at once (bulk signing), using an OTP (one-time-pin) as validation. • A signatory should be able to select each document and be able to sign them separately. • A signatory should also be able to select and sign multiple documents at once. • An OTP must be entered by the signatory as validation before the signatures are applied to the document/s.			
Different Electronic signature requirements	The system must make use of Advanced Electronic Signatures (AES) for customers that are required to sign collateral or any documentation related to transferring assets. Where the customer is not required to sign collateral, the use of a standard digital signature is acceptable. The CCT needs to define the digital signature policy to indicate what type of signature is required for what type of transaction. • An advanced electronic signature consists of a digital certificate confirming the identity of the applicant, with an added face-to-face verification mechanism, as well as 3-factor authentication, which includes[1]			

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature	Comply (Yes/No)	Comments	On-Premise or Cloud
	I) Biometrics, such as fingerprint and iris scan; ii) Pin, password, passphrase or secret question; and iii) Key, device • A citizen can make use of digital signatures for signing purposes, where no collateral is required. • If at least one document requires signing with an AES, the customer should make use of AES for all other documents within that contract pack to provide a consistent user experience.			
Digital Stamp	The system should create a digital stamp to reflect the signatory's signature. • The stamp should display the date, time, time zone, customer's full name, email address and mobile number as per the ECT act of 2002 • Where possible, the system needs to record the unique identifier/s for the device on which the customer/signatory is signing the document.			
	The system should be able to capture the customer's/signatory's location at the time of signing. • The customer's location can be captured based on the IP address for the device that the customer is using, alternatively, the customer can enable location services on their signing device. • The signatory's location is not to be displayed on the stamp but is still to be recorded in the metadata. • In the cases of cell phone signatures, it is recommended that the GPS coordinates of the cell phone be recorded as part of the metadata.			

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature	Comply (Yes/No)	Comments	On-Premise or Cloud
Tracking control	The system must allow for the signing progress to be tracked • Internal users of the system should be able to track any outstanding signatures, fields, etc. • Internal user can track who has or has not signed the documents and the outcome i.e., accept or reject. The version control and metadata in the Document Management system can be utilised to provide the tracking control.			
Integration with DMS and RMS	The system is to allow for documents to be appropriately stored. • Documents are to be pushed to the DMS (and filed under the correct taxonomy) and be stored on the DMS. • Document metadata is to also be recorded as part of this storage process. • Once all the signatures are received, the document needs to be converted to a record and saved in the RMS. The Case Management tool can be used in instances where cases were created to perform the document to record the transformation process.			
Expiry Date	The system should allow an expiration date for signing all required documents. • An internal user should be able to set a validity period during which the customer needs to sign the documentation, after which the documentation will expire. • Alternatively, the business rules in the Case Management system can be used to auto allocate the expiry dates. • The expiry period for OTP's will also have to be enforced and applied by the system if it forms part of the three-way validation process.			
	The system should send an appropriate reminder to a signatory if they do not complete the signing process once they commence their			

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature	Comply (Yes/No)	Comments	On-Premise or Cloud
	signing session • A reminder is to be sent out to the customer within a specified period, e.g. one hour after commencing their signing session, should they not complete the full signing process.			
	The system should allow for an internal user or an internal system to proceed with the cancellation of the document signing process. • In the case where documents need to be updated or redrawn, an internal user should be able to cancel the signing process until all prerequisites have been met.			
Customer rejection procedure	The system should allow for the customers/signatories to reject a document that requires signing. • The customer reserves the right to reject a document if they are unsatisfied with its contents and agreements therein. • In the case of multiple signatories, the rejection of a document by one of the signatories should cancel the signing process for all signatories. In such a case, all relevant parties to be notified of the cancellation/rejection, as well as the reason for rejection. The documents signed by signatories before the rejection should be void. This business rule is applicable for CAF and Co-debtors and Sureties. • A rejection update should be reflected on the DMS, where any relevant CCT stakeholders can access the information based on a reference number.			

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature	Comply (Yes/No)	Comments	On-Premise or Cloud
	The system should allow the customer/signatories to provide a reason for the rejection of a document. • Reasons should be provided as a selection list of predefined reasons from which the customer can choose. *These reasons will have to be defined by the CCT and signed off.* • A 'My reason is not listed' selection should be made available to the customer. If the customer/signatory selects this option, a free text box is to appear that allows them to capture additional detail. This text box is to have a character limit.			
Notes	The system should allow customers to add notes for changes they would like made. These notes can be entered in the case management system or the digital signature system but the motes should be reflected in the case management system. • Customer to be able to make notes on the document for amendment requests. • Customers should be allowed to make smaller, immaterial changes on their own which can be noted in an addendum to the contract. In this case, the customer should be able to continue with the signing process. The types of changes that the customer can be allowed to make are to be defined by respective Compliance and Legal stakeholders, as well as appropriate business rules. • Any changes that are made by the customer must also be pulled through and updated on the master record on the ERP system.			
Consolidated signature page	The system should have one consolidated signature page that needs to be signed, which represents all documents in the contract pack. • Signature page to reflect all documents that have been			

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature	Comply (Yes/No)	Comments	On-Premise or Cloud
	signed as well as all signatories that have signed (in the case of multiple signatories). • Should include a summary of the contract (amounts, etc.).			
	The system should have a consolidated signature page for every document that needs to be signed. • Once the documents have been signed, each document should have a page at the end where each signatory's signature will be reflected.			
Additional requirements	The system should also comply with the following requirements: • It should enable the user to sign the file types they typically use (e.g.PDF, DOC, DOCX, TXT, XML, etc.) • The system must integrate with the existing applications or those that might be used in the future, e.g., contract management, HR services. • The system should allow the CCT to brand the front end to reflect the corporate identity			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comments	On-Premise or Cloud

Workflow Engine functionality Workflow core elements are *events*, *triggers* and *routing*.	The Enterprise Workflow engine should be able to:
	• Manage and support event types:
	   o Create, Retrieve, Update or Delete a token
	   o Status Changes (may or may not include routing)
	   o Approval Activity (to include approved, declined, need more information etc.)
	   o Notifications
	   o eSignatures (associated with statements of certification, recognition of review or receipt, document management etc.)
	   o Legal statement of acceptance or contract - Policy issues related to e-signature and legally binding actions that may require a higher degree of authentication than normal processing.
	   o Batch Processes
	• Handle triggers:
	   o For each event type listed above
	   o Scheduled (specified date/time)
	   o Time-based intervals (window of time from an event or a scheduled trigger)
	   o Condition-based (i.e., a threshold reached)
	   o Manually launched
	   o Launch another workflow and or be launched by another workflow
	• Routing options:
	   o Parallel paths (two types)
	      ▪ Simultaneous routing path (may include approvals) where the triggers and events are not dependent upon each other until			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	they reach a common event. - Simultaneous routing path (may include approvals) where the triggers or events are dependent upon each other. ○ Conditional - Routing path to be defined by event or token attributes. ○ Ad-Hoc - Ability to escalate or re-route, add to, modify the routing process (with specific security permissions) - Ability to spawn localized or sub-process workflow routing within an event or trigger. - Support "black-box" routing where user manages trigger or event rather than allow workflow engine to route. - Manual routing of token - User-defined'			
Business Rules *Any enterprise workflow implementation must support all existing business rules within existing workflow systems or processes for those systems that will replace*	The workflow should support business rules with: - High level of complexity (more than 15 layers of dependent rules) - Ability to specify business rules for the token type, Role, User, metadata element, period (or any combination of above rules) etc. - Control overviews of workflow elements (based on modifiers specified above) (Example: a			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comments	On-Premise or Cloud

or re-factor their workflow to use the enterprise tool selected	specific business rule may define that watcher within ORG code X can only view the approval details of a token at their access level or below.)
	• Allow for ad-hoc modifications to business rules with defined security access.
	    ○ Currently, existing UWL workflows allow ad-hoc changes per token but do not allow those ad-hoc changes to be permanently applied as a new rule.
	• Ability to add business rules for a new token type or ORG/Role/User etc. without code changes (for example: with the use of an administrative user interface).
	• Ability to define escalation route(s), triggers or events for a specific token type or attribute.
	• Ability to provide business rule templates and copy/clone options of existing business rules.
	• Support the elimination of "empty" approval nodes on the workflow process.
	    ○ On set-up warning of a rule resulting in an empty approval event.
	    ○ When a contact removal results in an empty node a notification for reconciliation is generated.
	• Require tools and/or ability to build custom workflow solutions			

Notifications *Notifications provides a means of delivering a message to a set of recipients. The messages can be sent via various communication channels such as email, text message, tasks on a*	Workflow notifications should be able to: • Automatically notify individuals of tasks that they must perform. (Example: Approve token, review supporting information, respond to a request, etc.) via various mechanisms available through the workflow engine. • Automatically notify the creator of the token when task completion or outcome occurs (if specified by the user, role or business rule). • Support time-based triggered the notification.			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
user's calendar, phone call, etc.	• Record when system messages are sent and retain copies of sent messages. • Fetch data (any/all data sources) and include it in a notification message. • Create or include a hyperlink to a token defined destination within application or workflow engine. • Support delivery verification with a delivery receipt where needed/requested. • Security options for control of what type of messages can be sent via certain mechanisms (using reliable messaging that provides the underlying infrastructure for security). • Users should be able to configure notifications preferences to support their desired delivery method, display, etc.			
Audit & Historical tracking *Audit and history tracking enable organizations to construct a meaningful picture of what has or has not happened to a token. It also provides a greater level of accountability, allowing organizations to determine who made what changes when.*	The audit and tracking within the Enterprise Workflow tool should be able to: • When a token is passed through the workflow each status and activity change should allow for user comments. • Record the ID of the person or system who performs any activity in the system, as well as when and where the activity takes place (within what application or what portal, etc.). • Display a record of all the statuses a token goes through, and date/time the status of the token change. • Maintain and display a snapshot or version of the token at key routing points within the workflow. – This may be handled with other mechanisms such as "track changes" or capture only with certain data field/type changes. • Include notification information within the audit and history trail o Who, when (trigger), how and a copy of message text to be			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	included in the history.			

Presentation Layer *An enterprise workflow solution must be transparent to its users. Users need to know the status of tokens as they move through the workflow.*	The presentation layer needs of an enterprise solution must allow the following features:
	• Different portals for the different defined roles
	   o Options to extract data to provide to a system outside of workflow to deliver the information to the public or read-only views.
	• End-user applications may require their own separate presentation layer within their application.
	   o If the workflow tool is used across distinct applications, the user should have seamless navigation to the workflow features and functions.
	   o The workflow tool should allow for the branding of an individual application instance (i.e., logo, colours, etc.)
	• Information about the state of each token in the workflow is easily accessible.
	• List of tokens and their metadata that allow for sorting and filtering.
	• Profile of users or roles to allow for view definitions.
	• Graphical representation of workflow process and progress.
	• Provide colour-coding options for activities, status and flow as required for escalation and critical paths, etc. (Colour coding should enhance data, but not be the only way of defining status; there must be support for screen readers or colour-blind disabilities.)
	• Allow for control of notification preferences through the presentation layer (rather than through the workflow configuration). (Examples: Daily Digest, RSS, etc.)
	• Expose audit and history trail of the token (view to be defined at the user or role or application level).			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	• Presentation layer accessibility should be defined by workflow security settings and desired exposure (Web, desktop, embedded in another system, etc.).			

Security *Workflow security must support CCT's authentication and authorization standards. Authentication is a process of determining whether someone or something is, in fact, who or what it is declared to be Authorization determines a user's access to information, services, etc. with defined policies within an application.*	• Security for workflow should: • Integrate with single sign-on solutions as described in the document. • Integrate with RM&DM&CM roles. • Workflow roles must be mapped to security roles. • Support existing workflow roles within implemented workflow products and allow expansion to the current access (each workflow process may have its own set of roles and needs – see individual process requirements).
	  ○ Creator
	  ○ Stakeholder
	  ○ Approver
	  ○ Approver Delegate
	  ○ Leader
	  ○ Reviewer
	  ○ Watcher
	  ○ Viewer
	  ○ Public (for external exposure if desired) – Read Only
	 • Should have a standard set of security roles, but also allow configurable workflow roles.
	  ○ Workflow roles (as listed above) are to interact within the workflow engine. These should be configurable based on the needs of the specific process.
	 • Display different views for different security roles.
	 • Provide the ability to set an encryption or security level for a token type, token data element, extract files or attachment to meet confidentiality requirements for each unit.			

Integration Points. *See the integrations standards for the CCT that*	**Systems (Databases, etc.)** Enterprise Workflow engine may require integration with the following systems: • Enterprise Data Warehouse • Other Workflow Systems ○ SharePoint (HR, etc.)			

Core Functional Requirement Category	Core Functional Requirement	Comply (Yes/No)	Comments	On-Premise or Cloud

the system needs to adhere to for specific guidelines	o ERP solution)
	o Document Management system
	o Record Management system
	o Case Management System
	o Digital Signature system
	o etc.
	• Standards-based systems (APIs) (Business Applications examples below, not exhaustive)
	   o Procurement
	   o HR
	   o Finance
	   o Payroll
	   o Etc.
	• Security (as per CCT policies)
	   o Authentication
	   o Single Sign-on
	• The Internet (Web Services)			

Normalization of Data and Data Share	Workflow interactions should include: • Support the normalization of data within the various systems inside and outside of a UWL business unit utilizing workflow. o Token data elements should be normalized across systems within the workflow handoff. It should contain the required elements for sharing. • Facilitate token metadata share within workflow systems. • System verification of required approvals, data elements, etc. across multiple systems. • Data retrieval for display within workflow or application • Data retrieval for business rules processing of workflow, notifications, and display restrictions on the presentation layer.			
Technical Constraints	The Workflow system must allow for integration with other systems, business applications and workflows. • CCT systems and business applications will change over the next few years and might be implemented upon various technology frameworks. This environment should be supported.			

Core Functional Requirement Category	Functional Requirement – Search Engine	Comply (Yes/No)	Comments	On-Premise or Cloud

Functionality
The search function needs to provide a single interface to perform search requests across the Document, Record and Case management repositories, as well as other enterprise repositories if required, subject to the access and privilege rights of the users.
	Control
	
	• The search engine must be able to search for and retrieve a complete electronic folder, or folder part, and all its entries, and display all, and only, those entries in the context of that folder as a discrete group and a single retrieval process.).
	• The search engine must be able to search for, retrieve and display a set of electronic records taken from many different folders by specifying values to be searched for in electronic record metadata.
	• The search engine must be able to search for, retrieve and display an electronic folder by all implemented naming principles, including:
	   ○ a folder title text
	   ○ a folder numerical reference code.
	• Where full-text retrieval of record content is available, the search engine must ensure that a user who is not allowed access to an electronic record or folder cannot receive any information about the record or folder as a result of a full-text search.
	• When a search is completed, the solution identifies the latest version of the record, but all versions of the record are available for the user to select and view if have they the appropriate access rights.
	• Support a mix of metadata and content searches using controlled lists and combining search terms to conduct simple keyword and complex searches, using search terms such as Boolean terms, logical operators, broader and narrower terms, and proximity searches, as required.
	• The solution provides a help function to give guidance on searching and searching hints.
	• Retrieve information by searching the database using			

Core Functional Requirement Category	Functional Requirement – Search Engine	Comply (Yes/No)	Comments	On-Premise or Cloud

	at least the following parameters:
	  ○ Full text;
	  ○ Combined text and field;
	  ○ Keyword;
	  ○ File/document;
	  ○ Metadata field;
	  ○ Date document created/captured;
	  ○ Author of the document;
	  ○ Barcode;
	  ○ Location; and
	  ○ Classification scheme.
	• The solution retrieves information by searching across multiple databases, across all fields, from a single point of access, using the following minimum search functions:
	  ○ Full text
	  ○ Record format
	  ○ Last action
	  ○ Disposal action
	  ○ Disposition (status) of record, i.e., active, inactive, destroyed, archived, transferred
	  ○ Combined text and field
	  ○ Keyword
	  ○ Storage unit and record title and number
	  ○ Dates e.g., records created, captured, destroyed, etc.
	  ○ Author of record
	  ○ Barcode
	  ○ Location
	  ○ Classification scheme
	  ○ Unique identifier and
	  ○ Metadata element.
	• The search engine should allow the user to refine search criteria and results at a user level, based on operational needs.			

	Advanced Search and retrieval There are instances where it may be necessary to retrieve electronic records by content and to employ more sophisticated searching mechanisms to do so, including the use of a standard thesaurus. ○ The search engine must allow a RM Systems Administrator to specify any element of record			

Core Functional Requirement Category	Functional Requirement – Search Engine	Comply (Yes/No)	Comments	On-Premise or Cloud
	and folder metadata, and optionally full record content, that is to be indexed for future retrieval, and to define stop lists and must support the ability to change this configuration at a later date. ○ The search engine must be able to retrieve electronic records and electronic folders by an integrated search mechanism on both record content, and record and folder metadata. ○ The search engine must provide search mechanisms that offer both a browsing or graphical navigation approach within the folder structure and a direct searching approach. ○ The search engine must provide Boolean and probability-based full-text search and retrieval mechanisms and relevance ranking of retrieval results ○ The search engine must provide user assistance by query formulation, including the use of a controlled vocabulary system. ○ The search engine must support the sorting, printing and saving of search results in variable display formats. ○ Where (non-record) electronic documents are managed alongside electronic records in the same system, the search engine must be able to search for and retrieve both documents and records in an integrated manner. ○ The search engine must ensure that all retrieval operations are consistent with all access control restrictions so that an unauthorised user cannot access folders or records by use of an advanced search and retrieval mechanism. ○ The search engine should allow search requests to be made from outside the system, and support the ability to exchange search requests and search results with other systems			

Core Functional Requirement Category	Functional Requirement – Search Engine	Comply (Yes/No)	Comments	On-Premise or Cloud
	○ The search engine must allow users to save and re-use search parameters within the system against their user or team names.			
Indexing Customization *Most indices can be customized to better meet specific searching needs*	• Custom setup preferences must include: ○ the sensitivity of upper- and lower-case letters, ○ recognition of specific date formats, ○ the inclusion or exclusion of specific file types, and ○ Unicode compliance to identify and index foreign characters. • The inclusion of punctuation as a search operator, however, does not impact how a document is indexed. Derivations of a root term can also be queried by adding other characters such as asterisks, exclamation points and percentage signs. For example, a search for legal* would generate hits for legal, as well as legality, legalities, legalize, etc. Another example would be the addition of a tilde to the end of a word to search for all synonyms of that word. • The system should be able to search utilising multi-language ability to cater to the needs of South Africa. • The search engine needs to take the text in a document or record and break the text into searchable keywords through the process known as tokenization. • The system must support a free-text search that allows users to search every word in an entire document or a specified group of documents. • The solution must enable the RM System Administrator to configure default search options for end-users. • The solution enables the System Administrator to configure default search options for end-users.			

Core Functional Requirement Category	Functional Requirement – Search Engine	Comply (Yes/No)	Comments	On-Premise or Cloud
User Access	• The solution must allow the RM System Administrator or accredited RM practitioner to search within the disposal schedule. • The solution must withhold all or part of a search result, according to user access privileges and information security classification.			

Functional Requirement Category	Functional requirement - Publish	Comply (Yes/No)	Comments	On-Premise or Cloud

Access to external parties
The system must be able to manage access and the activities of third parties which have been subjected to online security procedures, and ensure that such processes do not impair the ability of the system to meet the core requirements of this specification.
	Access to the EDMS will be initially managed by the IT&S authentication and access procedures and systems. Once the user is allowed to access the RM&DM&CM environment, then:
	• The System Administrator or authorised user must assist in
	    o registering the user or third party as a user on the RM&DM&CM solution.
	    o Create user profiles that will govern the access rights of the user of third party.
	• The Access and security functionality as defined in the EDMS, RM&DM&CM and CMS must be adhered too.			

Access to Employees with URL *The system must provide the ability for CCT staff to*	Access to the EDMS will be initially managed by the IT&S authentication and access procedures and systems. Once the CCT staff member has logged into the CCT environment then the user will be allowed to access the RM&DM&CM			

Functional Requirement Category	Functional requirement - Publish	Comply (Yes/No)	Comments	On-Premise or Cloud
access documents via a URL or similar hyperlink object once the IT&S authentication and access have been granted	environment. then: • The system should allow the CCT staff member that has been provide with a document URL or hyperlink to automatically display to document that are referenced by the URL or Hyperlink. • The access rights of the user still need to be enforced and access must be blocked to a user if they do not have the right to view a document even if they have a hyperlink or URL. • The Access and security functionality as defined in the EDMS, RM&DM&CM and CMS must be adhered too.			
Creation of URL or document related hyperlink *The system must provide the users with the ability to copy a URL or hyperlink and forward the said link to a CCT staff member that will then be able to access the document via the URL or hyperlink subject to access rights and privileges*	The RM&DM&CM system must be capable of creation a document URL or hyperlink that can be utilised by users that have access rights to the RM&DM&CM to view the linked document on any device logged into the CCT environment. The system must: • Provide the user with the document URL or hyperlink that allow users to access the artefact directly without having to engage in search actions. • Provide the functionality for the document URL or hyperlink to be forwarded via e-mail from the RM&DM&CM system to any user that have access rights in the RM&DM&CM system.			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
Online security *The system must be able to manage digital records which have been subjected to*	**Encryption** • The system must be able to capture and register an encrypted record directly from an application capable of encryption.			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud

online security procedures, and ensure that such processes do not impair the ability of the system to meet the core requirements of this specification.	• The system must be able to store digital records in either encrypted or unencrypted form.
	• The system must support the use of metadata for digital records transmitted or captured in encrypted form, following the Recordkeeping Metadata Standard, including:
	   ○ the serial number or unique identifier of a digital certificate (where relevant);
	   ○ type of algorithm and level of encryption; and
	   ○ date and time stamps relating to encryption and/or decryption process.
	• The system must ensure that an encrypted record can only be accessed by those users associated with the relevant cryptographic key, in addition to other access controls allocated to the record.
	• The system must allow encryption to be removed when a record is captured or registered directly from another application.			

	Digital signatures
	• The system must be able to interface with digital signature technologies so that authentication metadata can be captured automatically.
	• The system must be able to check the validity of a digital signature at the time of registering a digital record.
	• The system must be able to store with the digital record:
	   ○ the digital signature associated with that record;
	   ○ the digital certificate authenticating the signature; and			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud

	o any other confirmation details, in such a way that they can be retrieved with the record, but without compromising the integrity of a private key.
	• The system must support the use of metadata for digital records transmitted or captured bearing digital signatures, following the Record and Document Management Metadata Standard. At a minimum, this metadata must note that a digital signature was authenticated.
	• The system must allow a RM System Administrator to configure the extent to which authentication metadata is routinely stored with the digital record. For example:
	    o retain the fact of successful authentication only;
	    o retain metadata about the authentication process; and
	    o retain all authentication metadata, including signatures.
	• The system must be able to demonstrate the continued integrity of a digitally signed record, irrespective of whether authorised changes have been made to its metadata.
	• During an export process, the system should be able to apply a digital signature to:
	    o a digital record; and/or
	    o a digital folder containing multiple records, in a manner that supports external authentication.			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud

	Authentication
	• The system must be able to store metadata about the process of authentication, including:
	  o the serial number or unique identifier of the digital certificate;
	  o the Registration and Certification Authority responsible for authentication; and
	  o the date and time of authentication.
	• The system must allow a configuration option to store authentication metadata:
	  o with the digital record to which it relates; or
	  o closely but separately linked to the digital record.
	• The system must be able to interface with PKI-based security technologies.			

	Cryptographic key management • The system must support the implementation of a key management plan. • The system must be able to maintain cryptographic keys for the life of the record with which they are associated. • The system must support the separate, secure storage of encrypted records and their associated decryption keys. • The system must be able to store digital certificates for encrypted records and digitally signed records and must warn a RM System Administrator of any certificates approaching expiry. • The system must automatically record the details of all online security processes in an audit trail. • The system must support date and time stamping for all			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	records subject to online security processes.			

	Digital watermarks
	• The system must be able to store records bearing digital watermarks.
	• The system must be able to store metadata about a digital watermark:
	   o with the digital record to which it relates; or
	   o closely but separately linked to the digital record.			

Workflow *The system may provide or be integrated with a workflow facility to support business and records management tasks in a controlled manner. The system must ensure that such processes do not impair its ability to meet the core requirements of this specification.* *Please note the request of the CCT IS&T division for the possible use of the RM&DM&CM workflow function to be utilised with other core applications. It does not form part of this section.*	**Workflow features** The system must have an enterprise-wide workflow capability that • must support workflows that consist of several procedural steps. • must allow standard workflows to be defined and maintained by a RM System Administrator. • not limit the number of steps for any given workflow. • must restrict the amendment of pre-programmed workflows to a RM System Administrator or other authorised user. • must record all changes to pre-programmed workflows in the audit trail. • must recognise both users and workgroups as participants. • must alert a user when a digital record has been sent to their in-tray for attention, and specify the attention required. • must support integration with electronic messaging facilities to notify users of records that may be waiting for their attention.			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	• must track the progress of a digital record or physical file through a workflow, so a user can determine its status in the process. • should provide the functionality for the automation of documentation-intensive business processes, including document handling, storage, manual entries as well as the verification of data to reduce time and resource wastage in performing manual indexing and verifications.			
	Workflow management The system must have an enterprise-wide workflow capability that • must not limit the number of workflows that can be defined. • must provide comprehensive reporting facilities to allow the monitoring of volumes, performance, and exceptions. • should provide workflow capabilities to manage case, document, record-centric workflows, including origination, maker-checker, approval, and rejection.			
	Workflow and records management The system must have an enterprise-wide workflow capability that ▪ must ensure digital records and folders remain correctly classified during a workflow process, retaining all links to other record plan entities. • must allow a digital document to be captured and registered during, or after, a workflow process. • must maintain the same access and security controls that apply to digital records			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	and physical files at all other times. • must ensure that workflow processes do not interfere with the scheduled disposal of digital records and physical files. • must notify a RM System Administrator that a digital record or physical file within a workflow process is due for disposal. • must ensure that digital records and physical files within the workflow process can be located using the standard search interface. • must support the progressive addition of metadata to digital records and physical files, as set out in the Record and Document Metadata Standards.			
Hybrid system management *The system must support the management of markers, physical folders and hybrid-folders in a manner consistent and fully integrated with the management of digital records and physical files.*	**Control and capture** • The system must support the management of markers, physical folders and hybrid folders in a manner consistent with the management of digital records and physical files. • The system must allow physical files to be classified with the same records classification tools in the same record plan used to manage digital folders. • The system must allow hybrid folders, which are part digital and part physical, to be classified with the same records classification tools in the same record plan used to manage digital folders. • The system must allow the physical and digital components of a hybrid folder to use the same title and unique identifier, but with appropriate indicators marking which is physical and which is digital.			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	• The system must enable the creation of a marker for each physical record registered in the system. • The system must allow markers to denote different types of physical record, allowing a user to enter the format as descriptive metadata. • The system must allow markers to be classified with the same records classification tools in the same record plan used to manage digital records. • The system should provide various library functionalities, such as check-in, check-out, auto-versioning, etc. • The system should provide the users with the ability to add notes and comments on cases, documents, records and folders for the users to collaborate on content seamlessly within the system.			
	Access and security • The system must ensure that the physical and digital components of a hybrid folder are allocated the same access and security controls. • The system must maintain the same access and security controls for markers, physical folders and hybrid folders that apply to digital records and folders at all times.			
	Disposal • The system must support the application of a disposal class to a physical folder, in a manner consistent with the management of digital folders. • The system must ensure that the physical and digital components of a hybrid			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	folder are allocated the same disposal class. • The system must ensure that the disposal action carried out on a hybrid folder is applied to both physical and digital components at the same time, taking into account the different processes required for destruction where applicable. • The system must apply disposal review decisions to both the physical and digital components of a hybrid folder. • The system must ensure that destruction or transfer of digital folder results in the destruction of any markers contained in that folder. • The system must maintain minimum metadata for destroyed items, including markers, physical folders and hybrid folders. • The system must alert the RM System Administrator to the existence and location of the physical component of a hybrid folder when such a folder is due for export or transfer. • The system must allow the export of physical folders and hybrid folders, retaining all associations with the digital component of the hybrid folder and the record plan once they are exported. • The system must allow the export of markers, retaining all associations with digital records and folders once they are exported. • The system must require a RM System Administrator to confirm that the physical component of a hybrid folder has been transferred, exported or destroyed before the digital component of the folder can be processed.			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	Searching and retrieval • The system must be able to retrieve markers, physical folders and hybrid folders along with digital records and folders, using the same search interface. • The system must ensure that retrieval of a digital folder also retrieves all markers associated with that folder. • The system must ensure that when a hybrid folder is retrieved, its physical and digital components are also retrieved.			
	Metadata • The system must support the use of metadata for markers, physical folders and hybrid folders, including inheritance of metadata consistent with inheritance by a digital record or folder. • The system must allow a different metadata element set to be configured for markers, physical folders and hybrid folders than that for digital records and folders so that metadata for physical entities can include physical location information. • The system must record changes to location metadata in the audit trail.			
	Scanning • The system should provide for the conversion of paper-based documentation to be digitised from a centralised or decentralised high-volume environment subject to the scanning strategy of the CCT. The conversion should allow for full text indexing and full text search of the documents by means of			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	optical character recognition (OCR). • The system should provide for fast conversion of high volumes and ensure quality of data is maintained • The system should be capable of identifying first and last pages by means of a barcode reader in a batch of documents to eliminate manual actions required to add or remove separator pages and have the ability to combine, separate, modify and import documents when required. • The system should provide for the automatic classification of documents imported in bulk. OCR should be utilised to read the text of documents and classify the document into metadata categories based on the information retrieved. • The system should provide Image enhancement technologies and techniques to ensure quality scanned images thereby reducing the need to rescan paper-based objects due to poor original quality results. • The system should allow for seamless integration with the workflow engine as per business requirements and ensure the document is captured in the DMS or stored as a record in the RMS with the appropriate metadata • The system should automatically read, index and extract data from documents and barcodes, irrespective of type and format			

Additional Functional Requirement Category	Additional Functional requirement	Comply (Yes/No)	Comments	On-Premise or Cloud
	• These requirements should be fulfilled in line with CCT security protocols as well as standards and legislation that applies. • .			

Non-Functionality Category	Non-Functional Requirements	Comply (Yes/No)	Comment
Security (*Degree to which a system protects artefacts, information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization*)	• Login / Access levels – The user configuration within the system should fulfil this NFR. • Create, Read, Update, and Delete (CRUD) levels - The user configuration within the system should fulfil this NFR. • Access permissions for application data may only be changed by the system's administrator and full audit traceability must be provided by the system reflecting all such interactions. • Separation of duties – the system should enforce the separation of duties of all security actions and processes involving independent actioner and approver roles. Due to the legal, governance and compliance requirements linked to Content management, the following NFR must be controlled by the system and not the general ICT policies: • Inactivity timeouts –the timeout durations, actions, and traceability requirements • System data backed up every *x* hours and copies stored in a secure off-site location. • Encryption (data in flight and at rest) – All external communications between the system's data server and clients must be encrypted and comply with the standards and regulations of the record management oversight agency. To comply with legislation and regulations, the system must satisfy the following requirements: • Confidentiality - Degree to which the system ensures that cases, documents, and records are accessible only to those authorized to have access. • Integrity - Degree to which the system and components prevent unauthorized access to, or modification of artefacts or data. • Non-repudiation - Degree to which actions or events can be proven to have taken place so that the events or actions cannot be repudiated later. • Accountability - Degree to which the actions of an entity can be traced uniquely to the entity. • Authenticity - Degree to which the identity of a subject or resource can be proved to be the one claimed. Required software and system must have Industry-strength Security with the following features & functionalities. • Definition of Users and Groups in the system • Access permissions on Folders, documents, and Data Classes • Multiple levels of access rights (Delete/Edit/View/None) • Grant users' privilege of creating users and groups • Secure login and passwords for each user • LDAP authentication and single sign-on support • Support for Data and Password Encryption		

Non-Functionality Category	Non-Functional Requirements	Comply (Yes/No)	Comment
	• Support for Digital Signatures and Biometric integration if these functions are not modules within the system but rather 3rd party add-ons • Supports SSL/HTTPS for secure transmission (Only TLS 1.2 or later supported as per cryptographic SOP)		
Audit (*Define the level of traceability for transactions required*)	• The system must maintain full traceability of transactions • User and transactional interactions must be time and date stamped by the system		
Capacity (*Provisioning for growth*)	• Throughput – the system must be able to handle 100000 transactions per hour as defined by the volume requirements during transactions peak times • Storage – (memory/disk) – the volume of data the system will page/persist at run time to disk • Year-on-year growth requirements (users, processing & storage) 10%		
Performance **(**The accomplishment of a given task measured against pre-set known standards of accuracy, completeness, cost, and speed.**)**	• Response times – Remote sites need to load, display and save documents and information within a variance of 25% than the times recorded at CCT HQ. • Processing times – functions, calculations, imports, exports • Bandwidth requirement – Due to cost to provide high-speed bandwidth connectivity, the response time and processing time NFR's must be accomplished with the minimal and not maximum bandwidth. • System automation – the system should auto-create and apply the appropriate taxonomy, file structure and archiving rules where possible to minimise human intervention. • Interoperability - The system must provide the ability to move information and artefacts easily between people, organisations and systems by providing standard API's to ERP, RM&DM&CM and packages. It is imperative that when information is shared between people and systems, its meaning is preserved from one context to another so that information is interpreted in the same way. That is, what was meant is the same as what is understood. This is the concept of "semantic" interoperability, which can be defined as: "The capability of two or more systems to communicate and exchange information, and for each system to be able to interpret the meaning of received information and to use it seamlessly with other data held by that system"		

Non-Functionality Category	Non-Functional Requirements	Comply (Yes/No)	Comment
Availability *(Uptime - Refers to the percentage of time that the infrastructure, system or a solution remains operational under normal circumstances to serve its intended purpose)*	• Operational availability – the system must be available during the hours of operation as well as the days as required by business that might differ from the standard IS&T availability policy. This would require the system to control these parameters independent from ICT. • Locality – the operational availability might differ from regional offices to HQ and the system should support site-specific availability parameters. • Replication – the system should support replication between remote or local Image Servers in the case where a cloud solution is not deployed.		
Object integrity (the overall accuracy, completeness, and consistency of data and objects)	• Data, artefacts, and information Integrity – the system should have the ability to ensure consistency of events, values, methods, measures, expectations and outcomes across data, artefacts, and information. • Compliance to data and information protection laws –the ability to apply and govern the application of compliance with, relevant information management regulation such as GDPR, POPIA. • Database recovery – the ability of the system to rebuild a consistent point in time set of data for the operating environment primarily for databases, but also for unstructured and configuration data sets. • Mean Time to Recovery – if broken, how much time is required to get the system back up again.		
Total Cost of Ownership (TCO) (an estimate of all the direct and indirect costs involved in acquiring and operating a system over a period)	• Reduced TCO by leveraging existing IT infrastructure - Products should be available on all industry-standard Operating Systems, Databases and Application Servers, and should be deployed on the platform of choice of the customer. Products should also be deployed on open-source platforms.		
Usability (Degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use)	• User Standards (**Look / Feel**) – Menu that provides access to all modules with the same look and feeling complying with Internationalization spellings, keyboards, etc. requirements • User error protection. The system needs to enforce data integrity, duplicate record validation, etc. to ensure that the system protects users against making errors. • Personalisation – the ability of the system to facilitate individual preference to be recorded and employed in all interactions without repeated user selection of preferences		

Non-Functionality Category	Non-Functional Requirements	Comply (Yes/No)	Comment
Resourcing (the reliance of the customer on software expertise to configure, customise or provide ongoing support)	• Ease of installation – Refers to the ability to install and configure the system by the customer's resources • Available resource – the availability of expert resources with their associated labour factor to successfully deploy the system • Continuous reliance on external support –to reduce the reliance on external parties, what is the cost and effort required to power the internal resources of the CCT to manage and support the system		
Documentation	• The availability and completeness of User Documentation • System Documentation to enable the CCT's technical staff to provide 1st line support function • Help? – the provision of a system integrated or online self-help facility • Training Material – complete and ease-of-use of materials for a user to refresh their knowledge or for new staff to familiarise themselves with the system.		
Disaster Recovery functionality	Required software and system must have Disaster Recovery functionality with the following features and functionalities: • Support for backing up and restoring of information for disaster recovery • Support for incremental and full Backups • Support for replicating data onto remote sites		
Third-Party Integration A comprehensive set of API's and SDK's should be available which should be used for unleashing the full power of both Business process management and document management system.	• The required solution should be component-based and can be deployed independently of each other by integration with any third-party core business application. • A comprehensive set of API's and SDK's should be available which can be used for unleashing the full power of the BPM and ECM / RM&DM&CM both. • Out of the box (OOTB) configuration using predesigned, pre-packaged templates, forms, workflows that are in place. • OOTB configuration time period to be 4-6 weeks		
Platform-independent DMS Web version	Required system and software should have Platform-independent DMS Web version • Required system and software should Expose standard Document Management features through a web interface • Required system and software should Use XML interfaces to internally communicate with the Transaction Server • Required system and software should be available on Windows, Linux and UNIX platforms.		

Schedule 15H - Pricing Instructions: OSM Recommended Retail Price List (Refer to paragraph 5.11 and 5.13 of the Pricing Instructions)
The Tenderer shall provide detailed and comprehensive OSM Recommended Retail Price Lists, for each OSM listed in the Price Schedules, in support of their Bid. The OSM price is the Original Software Manufacture's Recommended Retail Price at the closing date of the tender. CCT reserves the right to approach the Original Software Manufacturers directly for OSM Recommended Retail Price Lists, if required to ensure fair, equitable, transparent, competitive and cost-effective evaluation of the Bid. For goods the award of the tender will be based on the OSM(s) indicated by the tenderer, discount offered and mark-up percentages (%) the tenderer applies to a specific OSM's Recommended Retail Price List. The award for locally provided services (labour, etc.) will be based on the yearly fixed rates proposed by the Tenderer. The Tenderer must provide the relevant OSM Recommended Retail Price Lists.

SIGNED ON BEHALF OF TENDERER: . . . .

Schedule 15I – Technical Requirements: Technology Supported (Refer to paragraph 2.2.1.1.6 of the Eligibility Criteria and paragraph 13.5.1 of Technical Requirements)

The RM&DM&CM Solution should support modern technology based on table provided in Section 13 of the tender as a minimum.

The Tenderer must indicate in the column "Compliant Yes / No" whether the proposed solution adhere or can deliver on the specified technical requirement. Where the proposed solution doesn't meet the requirement or partially meets the requirement, the Tenderer must clearly indicate which functional requirements cannot be delivered on and provide a response or explanation how this situation can be mitigated. The Bid Evaluation Committee will assess whether the mitigation/ solution provided conforms to the scope required. The Tenderer can also add relevant information as an annexure to the tender response with a clear reference to the item the information refers to. Please refer to clause 2.3.7. Test for responsiveness on this matter.

PARADIGM/ CONTEXT	PROTOCOLS	SERIALISATION/ DATA FORMATS	COMPLY: YES/NO	COMMENTS/ MITIGATION	CLIENT REFERENCE
File Transfer	FTP (IETF Datatracker RFC959)				
ODBC					
Email	POP3 (IETF Datatracker - RFC1939) SMTP (IETF Datatracker - RFC5321) IMAP (IETF Datatracker - RFC3501) COAP (IETF Datatracker - RFC7252)				
REST SOAP	HTTP/1 (IETF Datatracker - RFC7230) HTTP/2 (IETF Datatracker - RFC7540) HTTP/3 (draft-ietf-quic-http-34) WebSockets (RFC6455)	JSON (IETF Datatracker - RFC8259) XML (W3 - Version 1.0, 1.1) YAML (YAML - Version 1.2)			
Message Queue Pub-Sub	Kafka Protocol AMQP (AMQP - 1.0, 0-9-1) ZMTP (RFC.ZeroMQ - 23/ZMTP) MQTT (OASIS - Version 5)				

SIGNED ON BEHALF OF TENDERER: . . . .

Schedule 15J – Project Requirements: Detailed Project Plan (Refer to Section13.5 in the Specifications)

Detailed Project Plan to be attached hereto, including the below deliverables.

Minimum Requirements for a project plan:

- Include the following activities:
    o Discovery and Planning
    o Design
    o Development
    o Testing
    o Deployment
    o Migration, Integration and Development
    o Input into Change Management
    o Enhanced three-month period of support post Deployment
- Contain milestones
- Contain Stage gates per phase and minimum requirements to pass
- Provide RACI Matrix taking into account dependencies on CCT

Information provided will not be used for evaluation purposes, but information purposes.

Schedule 15K– Cloud assessment criteria (Refer to paragraph 13.4.1 to paragraph 13.4.2.9 of Functional Requirements)

Where cloud offerings are proposed, please complete cloud assessment criteria in Table below:

Application Software Cost	
	Price (Year 1)
Original Software Cost	
Annual Maintenance/Licence Cost	
Rate Increase per year (%)	

INTERNAL Application Support and Enhancement cost for Resources - Per Year			
	Hours per month	FTE	Rate per hour
Bandwidth Cost External			
Contracted			
Additional			
Cloud Administrator			
Support			
Enhancements			
Finance Usage Monitoring & Monitoring Analyst			
Support			
Enhancements			
PaaS Cost if Applicable			
Contracted			
Additional			
IaaS Cost if Applicable			
Contracted			
Additional			
Database Programmer / Administrator			
Support			
Enhancements			
Business Analyst			
Support			
Enhancements			
Project Manager			
Support			
Enhancements			
Other			
Support			
Enhancements			
Rate increase/Year (%)			%

CONTRACTOR Application Support and Enhancement Resources - Per Year			
	Hours per month	FTE	Rate per hour
Project Manager			
Support			
Enhancements			
Business Analyst			
Support			
Enhancements			
Application Developer / Programmer			
Support			
Enhancements			
System Analyst			
Support			
Enhancements			
Application DBA			
Support			
Enhancements			
System Administrator			

Support			
Enhancements			
Database Administrator			
Support			
Enhancements			
Rate increase/Year (%)			%

Hosting Options		
	Price (Year 1)	Rate increase / Year (%)
Hybrid Cloud		
On Premise		
Cloud		

Alternative Costing (Leave 0 if not used)		
	Price (Year 1)	Rate increase / Year (%)

Information provided will not be used for evaluation purposes, but information purposes.

Schedule 15L – Technical Requirements: SPECIALISED TOOLS and RESOURCES Refer to section 13.5.6.2 of Specifications)

The Tenderer must indicate in the column "Compliant Yes / No" whether the proposed solution adhere or can deliver on the specified technical requirement. Where the proposed solution doesn't meet the requirement or partially meets the requirement, the Tenderer must clearly indicate which functional requirements cannot be delivered on and provide a response or explanation how this situation can be mitigated. The Bid Evaluation Committee will assess whether the mitigation/ solution provided conforms to the scope required. The Tenderer can also add relevant information as an annexure to the tender response with a clear reference to the item the information refers to. Please refer to clause 2.3.7. Test for responsiveness on this matter.

Item	Requirements	Applicable values	Comply Yes/No	Comment
1.	**File Analysis** Perform analytics on content stored in unstructured and semi-structured environments.	• On-premise/Cloud • Must connect to SharePoint, SAP and Windows File Share services as a minimum • Must index and analyze high volumes (>100TB) of data and large files (>300MB) • Must not slow down performance of source systems • Must operate between 95% and 99.9% uptime • Must be able to process high volumes without impacting the performance of the tool • Must provide in depth and visual reports on usage and management of files and metadata which can be aggregated for summary reports		
2.	**Data Classification** Perform analytics on content and assign/recommend metadata tags	• On premise/Cloud • Must connect to SharePoint, SAP and Windows File Share services as a minimum • Must index and analyze high volumes (>100TB) of data and large files (>300MB) • Must perform analysis of native metadata, custom metadata and file content to recommend metadata based on content of file • Must be able to manually amend metadata recommended • Must be able to automatically assign metadata to files as per automated recommendations or manual verifications		
3.	**Data Migration** Perform data migration of metadata and documents from structured, semi-structured and unstructured environments	• On premise/Cloud • Automated • Must connect to SharePoint, SAP and Windows File Share services as a minimum • Must not slow down performance of source systems • Must operate between 95% and 99.9% uptime • Must be able to process high volumes (>5TB per day) without impacting the performance of the tool • Must allow for schema identification and mapping from source to target • Must have built in data validation tools to report on migration success/errors • Must have reporting capabilities to provide automated and real time updates on migration processes • Must allow for data to be transformed		

	TENDER DOCUMENT GOODS AND SERVICES		
	SUPPLY CHAIN MANAGEMENT		
SCM - 542	Approved by Branch Manager: 03/04/2020	Version: 8	Page 169 of 66

TENDER NO:	**41S/2022/23**
TENDER DESCRIPTION:	**SUPPLY, INSTALLATION, SERVICE AND MAINTENANCE OF A RECORDS MANAGEMENT DOCUMENT MANANGEMENT AND CASE MANAGEMENT (RM&DM&CM) SOLUTION FOR THE CITY OF CAPE TOWN**
CONTRACT PERIOD:	**FROM DATE OF COMMENCEMENT OF CONTRACT UNTIL 31 MAY 2033**

VOLUME 3: DRAFT CONTRACT

TENDERER	
NAME of Company/Close Corporation or Partnership / Joint Venture/ Consortium or Sole Proprietor /Individual	
TRADING AS (if different from above)	

NATURE OF TENDER OFFER (please indicate below)	
Main Offer (see clause 2.2.11.1)	
Alternative Offer (see clause 2.2.11.1)	

VOLUME 3: DRAFT CONTRACT
(7) SPECIAL CONDITIONS OF CONTRACT

The following Special Conditions of Contract, referring to the National Treasury – Conditions of Contract (revised July 2010), are applicable to this Contract:

1. Definitions

Delete Clause 1.15 and substitute with the following

1.15   The word 'Goods' is to be replaced everywhere it occurs in the GCC with the phrase 'Goods and / or Services' which means all of the equipment, machinery, materials, services, products, consumables, etc. that the supplier is required to deliver to the purchaser under the contract. This definition shall also be applicable, as the context requires, anywhere where the words "supplies" and "services" occurs in the GCC.

Delete Clause 1.19 and substitute with the following

1.19   The word 'Order' is to be replaced everywhere it occurs in the GCC with the words 'Purchase Order' which means the official purchase order authorised and released on the purchaser's SAP System

Delete Clause 1.21 and substitute with the following:

1.21   'Purchaser' means the **City of Cape Town**. The address of the Purchaser is **12 Hertzog Boulevard, Cape Town, 8001**.

Add the following after Clause 1.25:

1.26   'Supplier' means any provider of goods and / or services with whom the contract is concluded

1.27   "Intellectual Property" means any and all intellectual property rights of any nature anywhere in the world whether registered, registerable or otherwise, including patents, trademarks, registered designs and domain names, applications for any of the foregoing, trade or business names, copyright and rights in the nature of copyright, design rights, rights in databases, know-how, trade secrets and any other intellectual property rights which subsist in computer software, computer programs, websites, documents, information, techniques, business methods, drawings, logos, instruction manuals, lists and procedures and particulars of customers, marketing methods and procedures and advertising literature, including the "look and feel" of any websites

3. General Obligations

Delete Clause 3.2 in its entirety and replace with the following clauses.

3.2   The parties will be liable to each other arising out of or in connection with any breach of the obligations detailed or implied in this contract, subject to clause 28.

3.3   All parties in a joint venture or consortium shall be jointly and severally liable to the purchaser in terms of this contract and shall carry individually the minimum levels of insurance stated in the contract, if any.

3.4   The parties shall comply with all laws, regulations and bylaws of local or other authorities having jurisdiction regarding the delivery of the goods and give all notices and pay all charges required by such authorities.

3.4.1   The parties agree that this contract shall also be subject to the CCT's Supply Chain Management Policy ('SCM Policy') that was applicable on the date the bid was advertised**, save that if the Employer adopts a new SCM Policy which contemplates that any clause therein would apply to the contract emanating from this tender, such clause shall also be applicable to that contract**. Please refer to this document contained on the CCT's website.

3.4.2   Abuse of the supply chain management system is not permitted and may result in cancellation of the contract, restriction of the supplier, and/or the exercise by the City of any other remedies available to it as described in the SCM Policy.

3.5   The **supplier** shall:

3.5.1   Arrange for the documents listed below to be provided to the Purchaser prior to the issuing of the order:

   a)   Proof of Insurance (Refer to Clause 11) or Insurance Broker's Warrantee
   b)   Letter of good standing from the Compensation Commissioner, or a licensed compensation insurer (Refer to Clause 11)
   c)   Initial delivery programme
   d)   Other requirements as detailed in the tender documents

3.5.2   Only when notified of the acceptance of the bid by the issuing of the order, the supplier shall commence with and carry out the delivery of the goods in accordance with the contract, to the satisfaction, of the purchaser

3.5.3   Provide all of the necessary materials, labour, plant and equipment required for the delivery of the goods including any temporary services that may be required

3.5.4   Insure his workmen and employees against death or injury arising out of the delivery of the goods

3.5.5   Be continuously represented during the delivery of the goods by a competent representative duly authorised to execute instructions;

3.5.6   In the event of a loss resulting in a claim against the insurance policies stated in clause 11, pay the first amount (excess) as required by the insurance policy

3.5.7   Comply with all written instructions from the purchaser subject to clause 18

3.5.8   Complete and deliver the goods within the period stated in clause 10, or any extensions thereof in terms of clause 21

3.5.9   Make good at his own expense all incomplete and defective goods during the warranty period

3.5.10 Pay to the purchaser any penalty for delay as due on demand by the purchaser. The supplier hereby consents to such amounts being deducted from any payment to the supplier.

3.5.11 Comply with the provisions of the OHAS Act & all relevant regulations.

3.5.12 Comply with all laws relating to wages and conditions generally governing the employment of labour in the Cape Town area and any applicable Bargaining Council agreements.

3.5.13 Deliver the goods in accordance with the contract and with all reasonable care, diligence and skill in accordance with generally accepted professional techniques and standards.

3.6   The **purchaser** shall:

3.6.1   Issue orders for the goods required under this Contract. No liability for payment will ensue for any work done if an official purchase order has not been issued to the supplier.

3.6.2   Make payment to the **supplier** for the goods as set out herein.

3.6.3   Take possession of the goods upon delivery by the supplier.

3.6.4   Regularly inspect the goods to establish that it is being delivered in compliance with the contract.

3.6.5   Give any instructions and/or explanations and/or variations to the supplier including any relevant advice to assist the supplier to understand the contract documents.

3.6.6   Grant or refuse any extension of time requested by the supplier to the period stated in clause 10.

3.6.7   Inspect the goods to determine if, in the opinion of the purchaser, it has been delivered in compliance with the contract, alternatively in such a state that it can be properly used for the purpose for which it was intended.

3.6.8   Brief the supplier and issue all documents, information, etc. in accordance with the contract.

5. Use of contract documents and information; inspection, copyright, confidentiality, etc.

Add the following after clause 5.4:

5.5   Copyright of all documents prepared by the supplier in accordance with the relevant provisions of the copyright Act (Act 98 of 1978) relating to contract shall be vested in the purchaser. Where copyright is vested in the supplier, the purchaser shall be entitled to use the documents or copy them only for the purposes for which they are intended in regard to the contract and need not obtain the supplier's permission to copy for such use. Where copyright is vested in the purchaser, the supplier shall not be liable in any way for the use of any of the information other than as originally intended for the contract and the purchaser hereby indemnifies the supplier against any claim which may be made against him by any party arising from the use of such documentation for other purposes.

The ownership of data and factual information collected by the supplier and paid for by the purchaser shall, after payment, vest with the purchaser

5.6   Publicity and publication
The supplier shall not release public or media statements or publish material related to the services or contract within two (2) years of completion of the services without the written approval of the purchaser, which approval shall not be unreasonably withheld.

5.7   Confidentiality
Both parties shall keep all information obtained by them in the context of the contract confidential and shall not divulge it without the written approval of the other party.

5.8   Intellectual Property

5.8.1   The supplier acknowledges that it shall not acquire any right, title or interest in or to the Intellectual Property of the Employer.

5.8.2   The supplier hereby assigns to the Employer, all Intellectual Property created, developed or otherwise brought into existence by it for the purposes of the contract, unless the Parties expressly agree otherwise in writing.

5.8.3   The supplier shall, and warrants that it shall:

5.8.3.1   not be entitled to use the Employer's Intellectual Property for any purpose other than as contemplated in this contract;

5.8.3.2   not modify, add to, change or alter the Employer's Intellectual Property, or any information or data related thereto, nor may the supplier produce any product as a result of, including and/or arising from any such information, data and Intellectual Property, and in the event that it does produce any such product, the product shall be, and be deemed in law to be, owned by the Employer;

5.8.3.3   not apply for or obtain registration of any domain name, trademark or design which is similar to any Intellectual Property of the Employer;

5.8.3.4   comply with all reasonable directions or instructions given to it by the Employer in relation to the form and manner of use of the Employer Intellectual Property, including without limitation, any brand guidelines which the Employer may provide to the supplier from time to time;

5.8.3.5   procure that its employees, directors, members and contractors comply strictly with the provisions of clauses 5.8.3.1 to 5.8.3.3 above; unless the Employer expressly agrees thereto in writing after obtaining due internal authority.

5.8.4 The supplier represents and warrants to the Employer that, in providing goods, services or both, as the case may be, for the duration of the contract, it will not infringe or make unauthorised use of the Intellectual Property rights of any third party and hereby indemnifies the Employer from any claims, liability, loss, damages, costs, and expenses arising from the infringement or unauthorised use by the supplier of any third party's Intellectual Property rights.

5.8.5 In the event that the contract is cancelled, terminated, ended or is declared void, any and all of the Employer's Intellectual Property, and any and all information and data related thereto, shall be immediately handed over to the Employer by the supplier and no copies thereof shall be retained by the supplier unless the Employer expressly and in writing, after obtaining due internal authority, agrees otherwise.

7. Performance Security

Delete clause 7.1 to 7.4 and replace with the following:

'Not Applicable. Tenderers must disregard **Form of Guarantee / Performance Security** and are not required to complete same.

8. Inspections, tests and analyses

Delete Clause 8.2 and substitute with the following:

8.2 If it is a bid condition that supplies to be produced or services to be rendered should at any stage during production or execution or on completion be subject to inspection, the premises of the bidder or contractor shall be open, at all reasonable hours, for inspection by a representative of the purchaser or an organisation acting on behalf of the purchaser.

10. Delivery and documents

Delete clauses 10.1 and 10.2 and replace with the following:

10.1 Delivery of the goods shall be made by the supplier in accordance with the terms specified in the contract. The time for delivery of the goods shall be the date as stated on the order. Orders for the supply and delivery of goods may be raised up until the expiry of a framework agreement bid, provided that the goods can be delivered within 30 days of expiry of the framework contract. All orders, other than for the supply and delivery of goods, must be completed prior to the expiry of the contract period.

10.2 The purchaser shall determine, in its sole discretion, whether the goods have been delivered in compliance with the contract, alternatively in such a state that it can be properly used for the purpose for which it was intended. When the purchaser determines that the goods have been satisfactorily delivered, the purchaser must issue an appropriate certification, or written approval, to that effect. Invoicing may only occur, and must be dated, on or after the date of acceptance of the goods.

11. Insurance

Add the following after clause 11.1:

11.2 Without limiting the obligations of the supplier in terms of this contract, the supplier shall effect and maintain the following additional insurances:

a) Public liability insurances, in the name of the supplier, covering the supplier and the purchaser against liability for the death of or injury to any person, or loss of or damage to any property, arising out of or in the course of this Contract, in an amount not less than **R20 million** for any single claim**;**

b) Motor Vehicle Liability Insurance, in respect of all vehicles owned and / or leased by the supplier, comprising (as a minimum) "Balance of Third Party" Risks including Passenger Liability Indemnity;

c) Registration / insurance in terms of the Compensation for Occupational Injuries and Disease Act, Act 130 of 1993**.** This can either take the form of a certified copy of a valid Letter of Good Standing issued by the Compensation Commissioner, or proof of insurance with a licenced compensation insurer, from either the bidder's broker or the insurance company itself (see **Proof of Insurance / Insurance Broker's Warranty** section in document for a pro forma version).

d)   Professional indemnity insurance providing cover in an amount of not less than R5 million in respect of each and every claim during the contract period.

In the event of under insurance or the insurer's repudiation of any claim for whatever reason, the CCT will retain its right of recourse against the supplier.

11.3   The supplier shall be obliged to furnish the CCT with proof of such insurance as the CCT may require from time to time for the duration of this Contract. Evidence that the insurances have been affected in terms of this clause, shall be either in the form of an insurance broker's warranty worded precisely as per the pro forma version contained in the **Proof of Insurance / Insurance Broker's Warranty** section of the document or copies of the insurance policies.

15. Warranty

Add to Clause 15.2:

15.2   This warranty for this contract shall remain valid for **twelve (12) months** from the date of installation and commissioning.

16. Payment

Delete Clause 16.1 in its entirety and replace with the following:

16.1   A monthly payment cycle will be the norm. All invoices which are dated on or before the 20th of a particular month will typically be paid between the 23rd and 26th of the following month. The supplier may submit a fully motivated application regarding more frequent payment to the Employer's Director: Expenditure for consideration. Requests for more frequent payments will be considered at the sole discretion of the Employer and is not a right in terms of this contract.

Delete Clause 16.2 in its entirety and replace with the following:

16.2   The supplier shall furnish the purchaser's Accounts Payable Department with an original tax invoice, clearly showing the amount due in respect of each and every claim for payment.

Add the following after clause 16.4

16.5   Notwithstanding any amount stated on the order, the supplier shall only be entitled to payment for goods actually delivered in terms of the Project Specification and Drawings, or any variations in accordance with clause 18. Any contingency sum included shall be for the sole use, and at the discretion, of the purchaser.

The CCT is not liable for payment of any invoice that pre-dates the date of delivery of the goods.

16.6   The purchaser will only make advanced payments to the supplier in strict compliance with the terms and details as contained on **Proforma Advanced Payment Guarantee** and only once the authenticity of such guarantee has been verified by the City's Treasury Department.

17. Prices

Add the following after clause 17.1

17.2   If as a result of an award of a contract beyond the original tender validity period, the contract execution will be completed beyond a period of twelve (12) months from the expiry of the original tender validity period, then the contract may be subject to contract price adjustment for that period beyond such twelve (12) months. An appropriate contract price adjustment formula will be determined by the Director: Supply Chain Management if such was not included in the bid documents.

17.3   If as a result of any extension of time granted the contract execution will be completed beyond a period of twelve (12) months from the expiry of the original tender validity period, then contract price adjustment may apply to that period beyond such twelve (12) months. An appropriate contract price adjustment formula will be determined by the Director: Supply Chain Management if such was not included in the bid documents.

17.4   The prices for labour rates and mark up price for the goods delivered are fixed and shall NOT be subject to contract price adjustment. The OSM price list will be subject to Rand/Dollar exchange rate fluctuations

17.5   If price adjustment for variations in the cost of plant and materials imported from outside of South Africa is provided for in the contract, such adjustment shall be based on the information contained in the schedule titled "**Price Basis for Imported Resources**" and as below. For the purposes of this clause the Rand value of imported Plant and Materials inserted on the schedule titled "**Price Basis for Imported Resources**" (column (F)) shall be the value in foreign currency (column (A)) converted to South African Rand (column (C)) by using the closing spot selling rate quoted by **CCT's** main banker, NEDBANK, on the Base Date (seven calendar days before tender closing date) rounded to the second decimal place (column(B)), to which shall be added any Customs Surcharge and Customs Duty applicable at that date (columns (D) and (E)).

17.5.1   Adjustment for variations in rates of exchange:

(a) The value in foreign currency inserted in column (A) shall be subject to clause (h) below when recalculating the Rand value.

(b) The rate of exchange inserted in column (B) shall be the closing spot selling rate quoted by Council's main banker, NEDBANK, on the Base Date, rounded to the second decimal place, subject to sub-paragraph (c) below.

(c) If the rate of exchange inserted by the Tenderer differs from the NEDBANK rate referred to above, then the NEDBANK rate shall apply and the Rand value in columns (C) and (F) shall be recalculated accordingly, without altering the price in the Price Schedule for the relevant items.

(d) If a tender from a supplier or sub-contractor provides for variations in rates of exchange, the Supplier may **only** claim for variations in rates of exchange if he binds the supplier or sub-contractor to the same provision to take out forward cover as described in sub-paragraph (e) below.

(e) The Supplier (or sub-contractor) shall within five working days from the date of placing a firm order on an overseas supplier, cover or recover forward by way of a contract with a bank which is an authorised foreign exchange dealer, the foreign exchange component of the cost of any imported Plant and Materials inserted by the Tenderer on the scheduled titled "**Price Basis for Imported Resources**".

(f) When the Supplier (or sub-contractor) so obtains forward cover, the Supplier shall immediately notify the CCT of the rate obtained and furnish the CCT with a copy of the foreign exchange contract note.

(g) Based on the evidence provided in sub-paragraph (f) above, the value in Rand inserted in column (C) of on the schedule titled "**Price Basis for Imported Resources** "shall be recalculated using the forward cover rate obtained, and any increase or decrease in the Rand value defined in this clause shall be adjusted accordingly, subject to sub-paragraph (h) below.

(h) The adjustments shall be calculated upon the value in foreign currency in the Supplier's (or sub-contractor's) **forward cover contract**, provided that, should this value exceed the value in foreign currency inserted in column (A) of on the schedule titled "**Price Basis for Imported Resources**", then the value in column (A) shall be used.

17.5.2   Adjustment for variations in customs surcharge and customs duty

(a) Any increase or decrease in the Rand value between the amounts of Customs Surcharge and Customs Duty inserted in on the schedule titled "**Price Basis for Imported Resources**" and those amounts actually paid to the Customs and Excise Authorities, which are due to changes in the percentage rates applicable or to the foreign exchange rate used by the authorities, shall be adjusted accordingly.

(b) The Tenderer shall state the Customs Duty Tariff Reference applicable to each item and the Supplier shall advise the CCT's Agent of any changes which occur.

17.5.3   Adjustment for variation in labour and material Costs

If the prices for imported Plant and Materials are not fixed, the Supplier shall in his Tender specify the formula for calculating Contract Price Adjustments normally used in the country of manufacture and the indices and relative proportions of labour and material on which his Tender prices are based. Evidence of the indices

applicable shall be provided with each claim. The indices applicable 42 days before contractual dispatch date from the factory will be used for the purposes of Contract Price Adjustment.

Failure to specify a formula in the Tender shall mean that the prices are fixed or shall be deemed to be fixed.

18. Contract Amendments

Delete the heading of clause 18 and replace with the following:

18.   Contract Amendments and Variations

Add the following to clause 18.1:

Variations means changes to the goods, extension of the duration or expansion of the value of the contract that the purchaser issues to the supplier as instructions in writing, subject to prior approval by the purchaser's delegated authority. Should the supplier deliver any goods not described in a written instruction from the purchaser, such work will not become due and payable until amended order has been issued by the purchaser.

20. Subcontracts

Add the following after clause 20.1:

20.2   The supplier shall be liable for the acts, defaults and negligence of any subcontractor, his agents or employees as fully as if they were the acts, defaults or negligence of the supplier.

20.3   Any appointment of a subcontractor shall not amount to a contract between the CCT and the subcontractor, or a responsibility or liability on the part of the CCT to the subcontractor and shall not relive the supplier from any liability or obligation under the contract.

21. Delays in the supplier's performance

Delete Clause 21.2 in its entirety and replace with the following:

21.2   If at any time during the performance of the contract the supplier or its sub-contractors should encounter conditions beyond their reasonable control which impede the timely delivery of the goods, the supplier shall notify the purchaser in writing, within 7 Days of first having become aware of these conditions, of the facts of the delay, its cause(s) and its probable duration. As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation, and may at his discretion extend the time for delivery.

Where additional time is granted, the purchaser shall also determine whether or not the supplier is entitled to payment for additional costs in respect thereof. The principle to be applied in this regard is that where the purchaser or any of its agents are responsible for the delay, reasonable costs shall be paid. In respect of delays that were beyond the reasonable control of both the supplier and the purchaser, additional time only (no costs) will be granted.

The purchaser shall notify the supplier in writing of his decision(s) in the above regard.

21.3   No provision in a contract shall be deemed to prohibit the obtaining of goods from a national department, provincial department, or a local authority.

22. Penalties

Delete clause 22.1 and replace with the following:

22.1   Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, as a penalty, a sum as stated herein for each day of the delay until actual delivery or performance.

The penalty for this contract shall be determined as a percentage on the purchase order request total for the services requested which failed to adhere to the performance level agreement as defined in clause 43.

22.2 The purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, financial penalties as contained on the **Preference Schedule** relaying to breaches of the conditions upon which preference points were awarded.

23. Termination

Add the following to the end of clause 23.1:

if the supplier fails to remedy the breach in term of such notice

Add the following after clause 23.7:

23.8 In addition to the grounds for termination due to default by the supplier, the contract may also be terminated:

23.8.1 Upon the death of the supplier who was a Sole Proprietor, or a sole member of a Close Corporation, in which case the contract will terminate forthwith.

23.8.2 The parties by mutual agreement terminate the contract.

23.8.3 If an Order has been issued incorrectly, or to the incorrect recipient, the resulting contract may be terminated by the purchaser by written notice

23.8.4 If a material irregularity vitiates the procurement process leading to the conclusion of the contract, rendering the procurement process and the conclusion of the resulting contract unfair, inequitable, non-transparent, uncompetitive or not cost-effective, provided the City Manager follows the processes as described in the purchasers SCM Policy.

23.8.5 After providing notice to the supplier, if the implementation of the contract may result in reputational risk or harm to the City as a result of (inter alia):

23.8.5.1   reports of poor governance and/or unethical behaviour;
23.8.5.2   association with known family of notorious individuals;
23.8.5.3   poor performance issues, known to the Employer;
23.8.5.4   negative social media reports; or
23.8.5.5   adverse assurance (e.g., due diligence) report outcomes.

23.9 If the contract is terminated in term of clause 23.8, all obligations that were due and enforceable prior to the date of the termination must be performed by the relevant party.

26.   Termination for insolvency

Delete clause 26.1 and replace with the following:

26.1 The purchaser may make either of the following elections to ensure its rights are protected and any negative impact on service delivery is mitigated:

26.1.1 accept a supplier proposal (via the liquidator) to render delivery utilising the appropriate contractual mechanisms; or

26.1.2 terminate the contract, as the liquidator proposed supplier is deemed unacceptable to the purchaser, at any time by giving written notice to the supplier (via the liquidator).

26.2 Termination will be without compensation to the supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the purchaser.

27. Settlement of Disputes

Amend clause 27.1 as follows:

27.1   If any dispute or difference of any kind whatsoever, with the exception of termination in term of clause 23.1(c), arises between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve such dispute or difference amicably, by mutual consultation.

Delete Clause 27.2 in its entirety and replace with the following:

27.2   Should the parties fail to resolve any dispute by way of mutual consultation, either party shall be entitled to refer the matter for mediation before an independent and impartial person appointed by the City Manager in accordance with Regulation 50(1) of the Local Government: Municipal Finance Management Act, 56 of 2003 – Municipal Supply Chain Management Regulations (Notice 868 of 2005). Such referral shall be done by either party giving written notice to the other of its intention to commence with mediation. No mediation may be commenced unless such notice is given to the other party.

Irrespective whether the mediation resolves the dispute, the parties shall bear their own costs concerning the mediation and share the costs of the mediator and related costs equally.

The mediator shall agree the procedures, representation and dates for the mediation process with the parties. The mediator may meet the parties together or individually to enable a settlement.

Where the parties reach settlement of the dispute or any part thereof, the mediator shall record such agreement and on signing thereof by the parties the agreement shall be final and binding.

Save for reference to any portion of any settlement or decision which has been agreed to be final and binding on the parties, no reference shall be made by or on behalf of either party in any subsequent court proceedings, to any outcome of an amicable settlement by mutual consultation, or the fact that any particular evidence was given, or to any submission, statement or admission made in the course of amicable settlement by mutual consultation or mediation.

28. Limitation of Liability

Delete clause 28.1 (b) and replace with the following:

(b)   the aggregate liability of the supplier to the purchaser, whether under the contract, in tort or otherwise, shall not exceed the sums insured in terms of clause 11 in respect of insurable events, or where no such amounts are stated, to an amount equal to twice the contract price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

Add the following after clause 28.1:

28.2   Without detracting from, and in addition to, any of the other indemnities in this contract, the supplier shall be solely liable for and hereby indemnifies and holds harmless the purchaser against all claims, charges, damages, costs, actions, liability, demands and/or proceedings and expense in connection with:

a)   personal injury or loss of life to any individual;
b)   loss of or damage to property;

arising from, out of, or in connection with the performance by the supplier in terms of this Contract, save to the extent caused by the gross negligence or wilful misconduct of the purchaser.

28.3   The supplier and/or its employees, agents, concessionaires, suppliers, sub-contractors or customers shall not have any claim of any nature against the purchaser for any loss, damage, injury or death which any of them may directly or indirectly suffer, whether or not such loss, damages, injury or death is caused through negligence of the purchaser or its agents or employees.

28.4   Notwithstanding anything to the contrary contained in this Contract, under no circumstances whatsoever, including as a result of its negligent (including grossly negligent) acts or omissions or those of its servants, agents or contractors or other persons for whom in law it may be liable, shall any party or its servants (in whose favour this constitutes a *stipulatio alteri*) be liable for any indirect, extrinsic, special, penal, punitive, exemplary or consequential loss or damage of any kind whatsoever, whether or not the loss was actually foreseen or reasonably foreseeable), sustained by the other party, its directors and/or servants, including but not limited to any loss of profits, loss of operation time, corruption or loss of information and/or loss of

contracts.

28.5   Each party agrees to waive all claims against the other insofar as the aggregate of compensation which might otherwise be payable exceeds the aforesaid maximum amounts payable.

31. Notices

Delete clauses 31.1 and 31.2 and replace with the following:

31.1   Any notice, request, consent, approvals or other communications made between the Parties pursuant to the Contract shall be in writing and forwarded to the addresses specified in the contract and may be given as set out hereunder and shall be deemed to have been received when:
a)   hand delivered – on the working day of delivery
b)   sent by registered mail – five (5) working days after mailing
c)   sent by email or telefax – one (1) working day after transmission

32. Taxes and Duties

Delete the final sentence of 32.3 and replace with the following:

In this regard, it is the responsibility of the supplier to submit documentary evidence in the form of a valid Tax Clearance Certificate issued by SARS to the CCT at the Supplier Management Unit located within the Supplier Management / Registration Office, 2nd Floor (Concourse Level), Civic Centre, 12 Hertzog Boulevard, Cape Town (Tel 021 400 9242/3/4/5).

Add the following after clause 32.3:

32.4 The **VAT registration** number of the City of Cape Town is **4500193497**.

ADDITIONAL CONDITIONS OF CONTRACT

Add the following Clause after Clause 34:

34 Conditions of Award
It is expected from the successful service provider to prove to the CCT that the solution he/she provides is capable of delivering on the requirements of the CCT. This will be done by means of a pilot project that will include all functionality of the solution to be tested on a legacy system chosen by the IT department of the CCT. Testing criteria will be set up by CCT IS&T officials and measured accordingly. If the bidder's solution does not meet the minimum expected results, the award will be offered to the bidder that is next on the evaluation list conducted by the CCT.

Following the bid adjudication process, an award will be made. The award will be dependent on the successful conclusion of the testing steps in section 13.4.10 **Refer to Specifications Section 13.4.5 (Requirements for the pilot), subject to the terms** listed immediately below:

a.   The successful service provider will be required to be accountable for the successful implementation of a pilot project in order to prove that the RM&DM&CM solution is able to meet the requirements of the CCT. **Refer to Specifications Section 13.4.5 (Requirements for the pilot)**

b.   All the work to be performed by the service provider will not be regarded as part of the project scope and will be costed for in **SCHEDULE B** of the Pricing Schedule in **Section 5.**

c.   The purchasing of any Software and Licences and the entering into of any further contractual agreements will be dependent on the successful implementation of the pilot project.

d.   Should it happen that the outcome of the pilot implementation is not successful, in that the product is not accepted from a functionality perspective and does not meet the requirements for the implementation of the pilot project, then the CCT reserves the right to cancel the award and to consider alternative bidders as per Clause **(2.1.5.3 Nomination of Alternative Bidder)**

e.   In such a case, where the service provider fails to successfully implement a pilot phase, the CCT will only be liable for payment on the portion of the work done up until the point of failure, and will NOT include any licensing or Software costs, including implementation and/or removal of

software pertaining to the RM&DM&CM solution.

35. Reporting Obligations.

35.1 The supplier shall complete, sign and submit with each delivery note, all the documents as required in the Specifications. Any failure in this regard may result in a delay in the processing of any payments.

36. OSM Certification

Tenderers must be authorised or accredited by the OSM or copyright holder to sell or distribute the software solution and manage any warranty processes and escalations as and when required. Alternatively, should the authorization / accreditation be from a distributor, then a proof of authorization authorizing the distributor to resell and/or authorize others by the OSM or copyright holder, must be submitted. Such authorisation or accreditation must be maintained for the duration of the contract.

37. Contract Performance Criteria.

37.1 The supplier shall adhere to the below Service Level Framework applicable to the RM&DM&CM Solution offered:

Note that a penalty percentage will be applied as per Table 37.1, Table 37.2 and Table 37.3 below if failure of adhering to the tabled metric occurs over a period of 3 consecutive incidences. City reserves the right to review each incident on its own merit concerning implementation of penalties. Credit note to be issued if penalty invoked in final year of tender.

The minimum service availability required is as follows:

Table 37.1: Implementation

Key performance indicator (KPI)	Response	Penalty (%) on Milestone Invoice
Quality of Solution delivery and Implementation	Delivery of solution, on-time in line with agreed timelines, meeting all set out functional requirements	4-6 months = 10%, 6-12 months = 20% + 12 months = 35%

Table 37.2: Maintenance

Key performance indicator (KPI)	Response	Target Announcements time	Target Resolution Time	Service Target	Reporting	Penalty (%) per purchase order
Security patches that form part of entire solution (Including 3rd party components, libraries or services installed as part of the software)	Announcement of security threat and plan to resolve.	1 Week	Monthly cycle	90%	Monthly report on response times	20%
Software faults	Announcement of software faults and plan to resolve.	1 Week	Monthly cycle	90%	Monthly report on planning	15%

| New features | Announcement of new features with impact plan. | 2 weeks | 3 months | 90% | Monthly report on response times | 5% |
| Upgrades | Announcement of new features with impact plan. | 1 month | 6 months | 90% | Monthly report on response times | 5% |

Table 37.3: Support

Key performance indicator (KPI)	Response	Severity	Target Response Time	Target Resolution Time	Service Target	Reporting	Route Cause Analysis Report	Penalty (%) per purchase order
Service Repair Support	Immediate and sustained effort, using all available resources until resolved. On-call procedures activated, vendor support invoked	Priority 1	15 minutes	4 Hours	90%	Monthly report on response times	4 Weeks after resolution	20%
Service Repair Support	Support Team responds immediately, assess the situation, may interrupt other staff working normal or moderate priority jobs for assistance	Priority 2	60 minutes	8 Hours	90%	Monthly report on response times	4 Weeks after resolution	15%
Service Repair Support	Respond using standard procedures and operating within normal supervisory management structures	Priority 3	2 business hours	12 Hours	90%	Monthly report on response times	4 Weeks after resolution	10%
Service Repair Support	Respond using standard operating procedures as time allows	Priority 4	4 business hours	2 Business Days	90%	Monthly report on response times	4 Weeks after resolution	5%

Table 37.4: Severity Classification: RM&DM&CM Solution

Priority Level	Description	Classification
Priority 1	Solution is down throughout the organisation	Critical
Priority 2	Solution is slow during peak times	High
Priority 3	Single department experiencing slow connection, work degradation	Moderate
Priority 4	Experiencing slow response from single application with no work degradation	Low

Priority Level	Description	Classification

(8) GENERAL CONDITIONS OF CONTRACT

(National Treasury - General Conditions of Contract (revised July 2010))

TABLE OF CLAUSES

1. Definitions

1. The following shall be interpreted as indicated:

   1.1 'Closing time' means the date and hour specified in the bidding documents for the receipt of bids.

   1.2 'Contract' means the written agreement entered into between the purchaser and the supplier, as recorded in the contract form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

   1.3 'Contract price' means the price payable to the supplier under the contract for the full and proper performance of his or her contractual obligations.

   1.4 'Corrupt practice' means the offering, giving, receiving, or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution.

   1.5 'Countervailing duties' are imposed in cases in which an enterprise abroad is subsidised by its government and encouraged to market its products internationally.

1.6 'Country of origin' means the place where the goods were mined, grown or produced or from which the services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembly of components, a commercially recognised new product results that is substantially different in basic characteristics or in purpose or utility from its components.

1.7 'Day' means calendar day.

1.8 'Delivery' means delivery in compliance with the conditions of the contract or order.

1.9 'Delivery ex stock' means immediate delivery directly from stock actually on hand.

1.10 'Delivery into consignee's store or to his site' means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the supplies are so delivered and a valid receipt is obtained.

1.11 'Dumping' occurs when a private enterprise abroad markets its goods on its own initiative in the RSA at lower prices than that of the country of origin, and which action has the potential to harm the local industries in the RSA.

1.12 'Force majeure' means an event beyond the control of the supplier, not involving the supplier's fault or negligence, and not foreseeable. Such events may include, but are not restricted to, acts of the purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

1.13 'Fraudulent practice' means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of any bidder, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the bidder of the benefits of free and open competition.

1.14 'GCC' means the General Conditions of Contract.

1.15 'Goods' means all of the equipment, machinery, and/or other materials that the supplier is required to supply to the purchaser under the contract.

1.16 'Imported content' means that portion of the bidding price represented by the cost of components, parts or materials which have been or are still to be imported (whether by the supplier or his subcontractors) and
which costs are inclusive of the costs abroad, plus freight and other direct importation costs such as landing costs, dock dues, import duty, sales duty or other similar tax or duty at the South African place of entry as well as transportation and handling charges to the factory in the Republic where the supplies covered by the bid will be manufactured.

1.17 'Local content' means that portion of the bidding price which is not included in the imported content, provided that local manufacture does take place.

1.18 'Manufacture' means the production of products in a factory using labour, materials, components and machinery, and includes other, related value-adding activities.

1.19 'Order' means an official written order issued for the supply of goods or works or the rendering of a service.

1.20 'Project site', where applicable, means the place indicated in bidding documents.

1.21 'Purchaser' means the organisation purchasing the goods.

1.22 'Republic' means the Republic of South Africa.

1.23 'SCC' means the Special Conditions of Contract.

1.24 'Services' means those functional services ancillaries to the supply of the goods, such as transportation and any other incidental services, such as installation, commissioning, provision of technical assistance, training, catering, gardening, security, maintenance, and other such obligations of the supplier covered under the contract.

1.25 'Written' or 'in writing' means handwritten in ink or any form of electronic or mechanical writing.

2. Application

2.1 These general conditions are applicable to all bids, contracts and orders, including bids for functional and professional services, sales, hiring, letting and the granting or acquiring of rights, but excluding immovable property, unless otherwise indicated in the bidding documents.

2.2 Where applicable, special conditions of contract are also laid down to cover specific supplies, services or works.

2.3 Where such special conditions of contract are in conflict with these general conditions, the special conditions shall apply.

3. General

3.1 Unless otherwise indicated in the bidding documents, the purchaser shall not be liable for any expense incurred in the preparation and submission of a bid. Where applicable, a non-refundable fee for documents may be charged.

3.2 With certain exceptions, invitations to bid are only published in the Government Tender Bulletin. The Government Tender Bulletin may be obtained directly from the Government Printer, Private Bag X85, Pretoria 0001, or accessed electronically from www.treasury.gov.za.

4. Standards

4.1 The goods supplied shall conform to the standards mentioned in the bidding documents and specifications.

5. Use of contract documents and information; inspection.

5.1 The supplier shall not, without the purchaser's prior written consent, disclose the contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the purchaser in connection therewith, to any person other than a person employed by the supplier in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for the purposes of such performance.

5.2 The supplier shall not, without the purchaser's prior written consent, make use of any document or information mentioned in GCC clause 5.1, except for purposes of performing the contract.

5.3 Any document, other than the contract itself, mentioned in GCC clause 5.1 shall remain the property of the purchaser and shall be returned (all copies) to the purchaser on completion of the supplier's performance under the contract if so required by the purchaser.

5.4 The supplier shall permit the purchaser to inspect the supplier's records relating to the performance of the supplier and to have them audited by auditors appointed by the purchaser, if so required by the purchaser.

6. Patent rights

6.1 The supplier shall indemnify the purchaser against all third-party claims of infringement of patent, trademark, or industrial design rights arising from the use of the goods or any part thereof by the purchaser.

7. Performance Security

7.1 Within 30 (thirty) days of receipt of the notification of contract award, the successful bidder shall furnish to the purchaser the performance security of the amount specified in the SCC.

7.2 The proceeds of the performance security shall be payable to the purchaser as compensation for any loss resulting from the supplier's failure to complete his obligations under the contract.

7.2 The performance security shall be denominated in the currency of the contract or in a freely convertible currency acceptable to the purchaser, and shall be in one of the following forms:

   a) a bank guarantee or an irrevocable letter of credit issued by a reputable bank located in the purchaser's country or abroad, acceptable to the purchaser, in the form provided in the bidding documents or another form acceptable to the purchaser; or
   b) a cashier's or certified cheque.

7.4 The performance security will be discharged by the purchaser and returned to the supplier not later than 30 (thirty) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless otherwise specified in the SCC.

8. Inspections, tests and analyses

8.1 All pre-bidding testing will be for the account of the bidder.

8.2 If it is a bid condition that supplies to be produced or services to be rendered should at any stage during production or execution or on completion be subject to inspection, the premises of the bidder or contractor shall be open, at all reasonable hours, for inspection by a representative of the Department or an organisation acting on behalf of the Department.

8.3 If there are no inspection requirements indicated in the bidding documents and no mention of such is made in the contract, but during the contract period it is decided that inspections shall be carried out, the purchaser shall itself make the necessary arrangements, including payment arrangements with the testing authority concerned.

8.4 If the inspections, tests and analyses referred to in clauses 8.2 and 8.3 show the supplies to be in accordance with the contract requirements, the cost of the inspections, tests and analyses shall be defrayed by the purchaser.

8.5 Where the supplies or services referred to in clauses 8.2 and 8.3 do not comply with the contract requirements, irrespective of whether such supplies or services are accepted or not, the cost in connection with these inspections, tests or analyses shall be defrayed by the supplier.

8.6 Supplies and services which are referred to in clauses 8.2 and 8.3 and which do not comply with the contract requirements may be rejected.

8.7 Any contract supplies may on or after delivery be inspected, tested or analysed and may be rejected if found not to comply with the requirements of the contract. Such rejected supplies shall be held at the cost and risk of the supplier, who shall, when called upon, remove them immediately at his own cost and forthwith substitute them with supplies which do comply with the requirements of the contract. Failing such removal, the rejected supplies shall be returned at the suppliers cost and risk. Should the supplier fail to provide the substitute supplies forthwith, the purchaser may, without giving the supplier further opportunity to substitute the rejected supplies, purchase such supplies as may be necessary at the expense of the supplier.

8.8 The provisions of clauses 8.4 to 8.7 shall not prejudice the right of the purchaser to cancel the contract on account of a breach of the conditions thereof, or to act in terms of Clause 23 of the GCC.

9. Packing

9.1 The supplier shall provide such packing of the goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the contract. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packing, case size and weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit.

9.2 The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the contract, including additional requirements, if any, specified in the SCC, and in any subsequent instructions ordered by the purchaser.

10. Delivery and documents

10.1 Delivery of the goods shall be made by the supplier in accordance with the terms specified in the contract. The details of shipping and/or other documents to be furnished by the supplier are specified in the SCC.

10.2 Documents to be submitted by the supplier are specified in the SCC.

11. Insurance

11.1 The goods supplied under the contract shall be fully insured, in a freely convertible currency, against loss or damage incidental to manufacture or acquisition, transportation, storage and delivery in the manner specified in the SCC.

12. Transportation

12.1 Should a price other than an all-inclusive delivered price be required, this shall be specified in the SCC.

13. Incidental Services

13.1 The supplier may be required to provide any or all of the following services, including additional services (if any) specified in the SCC:
(a) performance or supervision of on-site assembly, and/or commissioning of the supplied goods;
(b) furnishing of tools required for the assembly and/or maintenance of the supplied goods;
(c) furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied goods;
(d) performance or supervision or maintenance and/or repair of the supplied goods, for a period of time agreed by the parties, provided that this service shall not relieve the supplier of any warranty obligations under this contract; and
(e) training of the purchaser's personnel, at the supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied goods.

13.2 Prices charged by the supplier for incidental services, if not included in the contract price for the goods, shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the supplier for similar services.

14. Spare parts

14.1 As specified in the SCC, the supplier may be required to provide any or all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the supplier:
(a) such spare parts as the purchaser may elect to purchase from the supplier, provided that this election shall not relieve the supplier of any warranty obligations under the contract; and
(b) in the event of termination of production of the spare parts:

(i) Advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and

(ii) following such termination, furnishing at no cost to the purchaser, the blueprints, drawings, and specifications of the spare parts, if requested.

15. Warranty

15.1 The supplier warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The supplier further warrants that all goods supplied under this contract shall have no defect arising from design, materials, or workmanship (except when the design and/or material is required by the purchaser's specifications), or from any act or omission of the supplier, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.

15.2 This warranty shall remain valid for 12 (twelve) months after the goods, or any portion thereof, as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for 18 (eighteen) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise in the SCC.

15.3 The purchaser shall notify the supplier promptly, in writing, of any claims arising under this warranty.

15.4 Upon receipt of such notice, the supplier shall, within the period specified in the SCC and with all reasonable speed, repair or replace the defective goods or parts thereof, without costs to the purchaser.

15.5 If the supplier, having been notified, fails to remedy the defect(s) within the period specified in the SCC, the purchaser may proceed to take such remedial action as may be necessary, at the supplier's risk and expense and without prejudice to any other rights which the purchaser may have against the supplier under the contract.

16. Payment

16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in the SCC.

16.2 The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfilment of any other obligations stipulated in the contract.

16.3 Payments shall be made promptly by the purchaser, but in no case later than 30 (thirty) days after submission of an invoice or claim by the supplier.

16.4 Payment will be made in Rand unless otherwise stipulated in the SCC.

17. Prices

17.1 Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices tendered by the supplier in his bid, with the exception of any price adjustments authorized in the SCC or in the purchaser's request for bid validity extension, as the case may be.

18. Contract Amendments

18.1 No variation in or modification of the terms of the contract shall be made except by written amendment signed by the parties concerned.

19. Assignment

19.1 The supplier shall not assign, in whole or in part, its obligations to perform under the contract, except with the purchaser's prior written consent.

20. Subcontracts

20.1 The supplier shall notify the purchaser in writing of all subcontracts awarded under this contract if not already specified in the bid. Such notification, in the original bid or later, shall not relieve the supplier from any liability or obligation under the contract.

21. Delays in the supplier's performance

21.1 Delivery of the goods and performance of services shall be made by the supplier in accordance with the time schedule prescribed by the purchaser in the contract.

21.2 If at any time during the performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at his or her discretion extend the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the parties by amendment of contract.

21.3 No provision in a contract shall be deemed to prohibit the obtaining of supplies or services from a national department, provincial department, or a local authority.

21.4 The right is reserved to procure, outside of the contract, small quantities of supplies; or to have minor essential services executed if an emergency arises, or the supplier's point of supply is not situated at or near the place where the supplies are required, or the supplier's services are not readily available.

21.5 Except as provided under GCC Clause 25, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of penalties, pursuant to GCC Clause 22, unless an extension of time is agreed upon pursuant to GCC Clause 21.2 without the application of penalties.

21.6 Upon any delay beyond the delivery period in the case of a supplies contract, the purchaser shall, without cancelling the contract, be entitled to purchase supplies of a similar quality and up to the same quantity in
substitution of the goods not supplied in conformity with the contract and to return any goods delivered later at the supplier's expense and risk, or to cancel the contract and buy such goods as may be required to complete the contract and, without prejudice to his other rights, be entitled to claim damages from the supplier.

22. Penalties

22.1 Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods or to perform the services within the period(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, as a penalty, a sum calculated on the delivered price of the delayed goods or unperformed services, using the current prime interest rate, calculated for each day of the delay until actual delivery or performance. The purchaser may also consider termination of the contract pursuant to GCC Clause 23.

23. Termination for default

23.1 The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:

   (a) if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, or within any extension thereof granted by the purchaser pursuant to GCC Clause 21.2;
   (b) if the supplier fails to perform any other obligation(s) under the contract; or
   (c) if the supplier, in the judgment of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

23.2 In the event the purchaser terminates the contract in whole or in part, the purchaser may procure, upon such terms and in such manner as it deems appropriate, goods, works or services similar to those undelivered, and the supplier shall be liable to the purchaser for any excess costs for such similar goods, works or services. However, the supplier shall continue performance of the contract to the extent not terminated.

23.3 Where the purchaser terminates the contract in whole or in part, the purchaser may decide to impose a restriction penalty on the supplier by prohibiting such supplier from doing business with the public sector for a period not exceeding 10 years.

23.4 If a purchaser intends imposing a restriction on a supplier or any person associated with the supplier, the supplier will be allowed a time period of not more than 14 (fourteen) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated 14 (fourteen) days the purchaser may regard the intended penalty as not objected against and may impose it on the supplier.

23.5 Any restriction imposed on any person by the Accounting Officer/Authority will, at the discretion of the Accounting Officer/Authority, also be applicable to any other enterprise or any partner, manager, director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which enterprise or person the first-mentioned person is or was, in the opinion of the Accounting Officer/Authority, actively associated.

23.6 If a restriction is imposed, the purchaser must, within 5 (five) working days of such imposition, furnish the National Treasury with the following information:
   (i)   the name and address of the supplier and/or person restricted by the purchaser;
   (ii)   the date of commencement of the restriction;
   (iii) the period of restriction; and
   (iv)   the reasons for the restriction.

   These details will be loaded in the National Treasury's central database of suppliers or persons prohibited from doing business with the public sector.

23.7 If a court of law convicts a person of an offence as contemplated in sections 12 or 13 of the Prevention and Combating of Corrupt Activities Act, Act 12 of 2004, the court may also rule that such person's name be endorsed on the Register for Tender Defaulters. When a person's name has been endorsed on the Register, the person will be prohibited from doing business with the public sector for a period of not less than five years and not more than 10 years. The National Treasury is empowered to determine the period of restriction, and each case will be dealt with on its own merits. According to section 32 of the Act the Register must be open to the public. The Register can be perused on the National Treasury website.

24. Anti-dumping and countervailing duties and rights

24.1 When, after the date of bid, provisional payments are required, or anti-dumping or countervailing duties are imposed, or the amount of a provisional payment or anti-dumping or countervailing right is increased in respect of any dumped or subsidised import, the State is not liable for any amount so required or imposed, or for the amount of any such increase. When, after the said date, such a provisional payment is no longer required or any such anti-dumping or countervailing right is abolished, or where the amount of such provisional payment or any such right is reduced, any such favourable difference shall, on demand, be paid forthwith by the contractor to the State, or the State may deduct such amounts from moneys (if any) which may otherwise be due to the contractor in regard to supplies or services which he or she delivered or rendered, or is to deliver or render in terms of the contract or any other contract or any other amount which may be due to him or her.

25. Force majeure

25.1 Notwithstanding the provisions of GCC Clauses 22 and 23, the supplier shall not be liable for forfeiture of its performance security, damages, or termination for default if, and to the extent that, his delay in performance or other failure to perform his obligations under the contract is the result of an event of force majeure.

25.2 If a force majeure situation arises, the supplier shall notify the purchaser promptly, in writing, of such condition and the cause thereof. Unless otherwise directed by the purchaser in writing, the supplier shall continue to perform its obligations under the contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the force majeure event.

26. Termination for insolvency

26.1 The purchaser may at any time terminate the contract by giving written notice to the supplier if the supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the purchaser.

27. Settlement of Disputes

27.1 If any dispute or difference of any kind whatsoever arises between the purchaser and the supplier in connection with or arising out of the contract, the parties shall make every effort to resolve such dispute or difference amicably, by mutual consultation.

27.2 If, after 30 (thirty) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of his intention to commence with mediation. No mediation in respect of this matter may be commenced unless such notice is given to the other party.

27.3 Should it not be possible to settle a dispute by means of mediation, it may be settled in a South African court of law.

27.4 Mediation proceedings shall be conducted in accordance with the rules of procedure specified in the SCC.

27.5 Notwithstanding any reference to mediation and/or court proceedings herein,
(a) the parties shall continue to perform their respective obligations under the contract unless they otherwise agree; and
(b) the purchaser shall pay the supplier any monies due to the supplier.

28. Limitation of Liability

28.1 Except in cases of criminal negligence or wilful misconduct, and in the case of infringement pursuant to Clause 6:
(a) the supplier shall not be liable to the purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier to pay penalties and/or damages to the purchaser; and
(b) the aggregate liability of the supplier to the purchaser, whether under the contract, in tort or otherwise, shall not exceed the total contract price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

29. Governing language

29.1 The contract shall be written in English. All correspondence and other documents pertaining to the contract that is exchanged by the parties shall also be written in English.

30. Applicable Law

30.1 The contract shall be interpreted in accordance with South African laws, unless otherwise specified in the SCC.

31. Notices

31.1 Every written acceptance of a bid shall be posted to the supplier concerned by registered or certified mail, and any other notice to him shall be posted by ordinary mail, to the address furnished in his bid or to the address notified later by him in writing; and such posting shall be deemed to be proper service of such notice.

31.2 The time mentioned in the contract documents for performing any act after such aforesaid notice has been given, shall be reckoned from the date of posting of such notice.

32. Taxes and Duties

32.1 A foreign supplier shall be entirely responsible for all taxes, stamp duties, licence fees, and other such levies imposed outside the purchaser's country.

32.2 A local supplier shall be entirely responsible for all taxes, duties, licence fees, etc., incurred until delivery of the contracted goods to the purchaser.

32.3 No contract shall be concluded with any bidder whose tax matters are not in order. Prior to the award of a bid the Department must be in possession of a tax clearance certificate submitted by the bidder. This certificate must be an original issued by the South African Revenue Services.

33. National Industrial Participation (NIP) Programme

33.1 The NIP Programme administered by the Department of Trade and Industry shall be applicable to all contracts that are subject to the NIP obligation.

34 Prohibition of Restrictive practices

34.1 In terms of section 4 (1) (b) (iii) of the Competition Act, Act 89 of 1998, as amended, an agreement between or concerted practice by firms, or a decision by an association of firms, is prohibited if it is between parties in a horizontal relationship and if a bidder(s) is/are or a contractor(s) was/were involved in collusive bidding (or bid rigging).

34.2 If a bidder(s) or contractor(s), based on reasonable grounds or evidence obtained by the purchaser, has/have engaged in the restrictive practice referred to above, the purchaser may refer the matter to the Competition Commission for investigation and possible imposition of administrative penalties as contemplated in the Competition Act, Act 89 of 1998.

34.3 If a bidder(s) or contractor(s) has/have been found guilty by the Competition Commission of the restrictive practice referred to above, the purchaser may, in addition and without prejudice to any other remedy provided for, invalidate the bid(s) for such item(s) offered, and/or terminate the contract in whole or part, and/or restrict the bidder(s) or contractor(s) from conducting business with the public sector for a period not exceeding 10 (ten) years and/or claim damages from the bidder(s) or contractor(s) concerned.

(9) FORM OF GUARANTEE / PERFORMANCE SECURITY

NOT APPLICABLE TO THIS TENDER

(10) FORM OF ADVANCE PAYMENT GUARANTEE

NOT APPLICABLE TO THIS TENDER

(10.1) ADVANCE PAYMENT SCHEDULE

NOT APPLICABLE TO THIS TENDER

(11) OCCUPATIONAL HEALTH AND SAFETY AGREEMENT

AGREEMENT MADE AND ENTERED INTO BETWEEN THE CITY OF CAPE TOWN (HEREINAFTER CALLED THE "CCT") AND

……………………..................……………………………….......Supplier/Mandatary/Company/CC Name)

IN TERMS OF SECTION 37(2) OF THE OCCUPATIONAL HEALTH AND SAFETY ACT, 85 OF 1993 AS AMENDED.

I, …………………………………………..…………………………….............…………………………., representing

………………………………………………………………………...……………………………., as an employer in its own right, do hereby undertake to ensure, as far as is reasonably practicable, that all work will be performed, and all equipment, machinery or plant used in such a manner as to comply with the provisions of the Occupational Health and Safety Act (OHSA) and the Regulations promulgated thereunder.

I furthermore confirm that I am/we are registered with the Compensation Commissioner and that all registration and assessment monies due to the Compensation Commissioner have been fully paid or that I/We are insured with an approved licensed compensation insurer.

COID ACT Registration Number: ………………………………………………………………………………..

OR Compensation Insurer: .... Policy No.: ....

I undertake to appoint, where required, suitable competent persons, in writing, in terms of the requirements of OHSA and the Regulations and to charge him/them with the duty of ensuring that the provisions of OHSA and Regulations as well as the Council's Special Conditions of Contract, Way Leave, Lock-Out and Work Permit Procedures are adhered to as far as reasonably practicable.

I further undertake to ensure that any subcontractors employed by me will enter into an occupational health and safety agreement separately, and that such subcontractors comply with the conditions set.

I hereby declare that I have read and understand the Occupational Health and Safety Specifications contained in this tender and undertake to comply therewith at all times.

I hereby also undertake to comply with the Occupational Health and Safety Specification and Plan submitted and approved in terms thereof.

Signed at ....on the....................................day of................................20….

_____   _____
Witness   **Mandatary**

Signed at .... on the..................................day of....................................20 ....

_____   _____
Witness   for and on behalf of
                                                      City of Cape Town

(12) INSURANCE BROKER'S WARRANTY (PRO FORMA)

Logo

Letterhead of supplier's Insurance Broker

Date _____

CITY OF CAPE TOWN
City Manager
Civic Centre
12 Hertzog Boulevard
Cape Town
8000

Dear Sir

TENDER NO.:

TENDER DESCRIPTION:

NAME OF SUPPLIER: _____

I, the undersigned, do hereby confirm and warrant that all the insurances required in terms of the abovementioned contract have been issued and/or in the case of blanket/umbrella policies, have been endorsed to reflect the interests of the CITY OF CAPE TOWN with regard to the abovementioned contract, and that all the insurances and endorsements, etc., are all in accordance with the requirements of the contract.

I furthermore confirm that all premiums in the above regard have been paid.

Yours faithfully

Signed: _____

For: _____ (Supplier's Insurance Broker)

(13) SPECIFICATION(S)

13.1 INTRODUCTION AND BACKGROUND

As part of a digitisation drive by the City of Cape Town (CCT), certain foundational technologies were identified to be implemented first to provide the foundation for future initiatives that will form part of their digital strategy and aspirations. The initial technologies would also establish the foundations to enable the future loose coupling of applications. Records Management & Document Management & Case Management solutions as well as an imbedded Workflow Management solution implementation were selected as one of the foundational tenders to be published first.

Although the name of the tender refers to Document Management and Records Management, the term Records Management and Documents Management (RM&DM&CM) are utilised widely in all the guidance and standards documentation. RM&DM&CM refers to the management of records/ documents and case management for an organization throughout the document or records-life cycle. The activities in this RM&DM&CM solution include the systematic and efficient control and flow of the creation, maintenance, and destruction of the records along with the business transactions associated with these actions.

The current Records and Document management operations focus mainly on three areas namely Records Management, Case Management, Document Management in SAP and Document Management in SharePoint with the focus on SharePoint sites named TeamSite, MySite, and CTApps. In addition to SAP and SharePoint, the CCT is utilising a file server, FS01, for the storage of technical documentation.

Departmental Shared folders and project shared folders stored on the file server (FS01) that are not incorporated in the TeamSite and MySite areas, do not currently form part of the unstructured information that is controlled and managed via the CCT's document management protocols.

The full scope of the tender would be stipulated in the technical requirements below.

In the case of the CCT, the term Record Management and Document Management or RM&DM&CM would imply the inclusion of Case Management.

13.2 GOAL AND OBJECTIVES

The project seeks to fulfil the goals listed below for the CCT by implementing a world-class Record Management and Document Management System (RM&DM&CM) that also cater for case management, coupled with a Workflow management solution that can be used as an Enterprise-wide application. The goals are:
- Develop an integrated central document and records repository and case management facility.
- Improve employee RM&DM&CM
- Improve audits and controls.
- Improve the flow of information in the organization.
- Increase access, knowledge sharing and collaboration.
- Reduce the storage of duplicate documents.
- Protect sensitive information as per legislative requirements.

The objectives of this project are:
- To implement the base of the business in RM&DM&CM of Records Management and Documents storage for all solutions.
- To enable conversion of paper records to electronic records, thereby enabling all the advantages of a paper-free office.
- To enable the business to register, manage and process records and documents quickly and easily in line with dynamically updatable classification systems and systems and procedures in an integrated manner, e.g. from email applications and desktop to the RM&DM&CM system.
- To enable fast and secure access to records, documents, and cases.
- Integration with the workflow management tool to efficiently control the records management processes.
- To enable users to capture data only once, store it, distribute, and manage it resulting in the effective sharing of the data and artefacts across the enterprise.
- Each data element to have a trustee accountable for data quality.

- All data to be classified and protected from unauthorised use and disclosure.
- Demonstrate the value of the tool to deliver a return on investment to the organization with minimal costs to the residence of the CCT.
- To find a solution, if possible, where the RM&DM&CM workflow function can be utilised as an enterprise-wide solution to manage workflows that are not RM&DM&CM related.

This tender provides for the creation of the technology layer that will enable Enterprise Content Management (ECM) or Intelligent Information Management (IIM) that looks beyond this technology layer to ensure people, process and technology are working together in harmony as per the specified functional requirements.

13.2   SCOPE CLARIFICATION

The high-level scope of this tender is to provide an integrated solution that fulfils the Document and Records Management functionality of the CCT. In addition to this requirement, the solution should also cater for the integration of a Case Management solution with the addition of a digital signature solution. The CCT also requires that the Workflow Engine should be capable to be utilised as an Enterprise-wide workflow engine.

In addition to the above-mentioned requirements, the need for a digital signature, advanced search Engine and publish modules as defined in the functional requirements below.

The emphasis of the various Document and Records management functions focus strongly on the provision of an integrated solution.

The Document Management solution and the Record Management Solution can be from a single or two vendors, but these modules should be integrated and fulfil the functional requirements for these modules as stipulated in this document. The integration also includes integrations with any legacy systems or future systems that will come online during the RM&DM&CM implementation.
.
The Case Management module/system and the Digital Signature module/system should also integrate with the integrated RM&DM&CM solution and the current legacy systems or future systems.

13.2.1 IN SCOPE

13.2.1.1 Technical Perspective
1. Development of existing SAP Records and Case Management (SAP RCM) and SharePoint in scope sites and applications.
2. Integrated with legacy systems within the CCT application landscape in instances where the application creates and or depends on documentation and records.
3. Migration of the existing SAP-based Records and Cases as well as SharePoint and FS01 documents, legacy system documentation as well as the associated metadata where applicable.
4. Migration and classification of existing SAP ECC6 documents.
5. As part of the RM&DM&CM solution, enable and Implement an Enterprise-wide Electronic Signature and a Case Management System.
6. It is recommended that the Workflow component of the awarded solution is considered as a broader enterprise workflow solution for the City outside of just the Records and Document Management solution.
7. The applications landscape will change over the next 5 years and to ensure continued system integration and compliance the RM&DM&CM vendor needs to amend the workflow and initiate the system integrations where needed as per the CCT integration principles (see the Integration section).
8. Setup and configuring of the Scanning Equipment including the specifications required from outsourced scanning facilities to align with the CCT's RM&DM&CM requirements.
9. Records and Document Publishing to the Internet.

13.2.1.2   Business Perspective
1. Provide business user Training to staff on the new solution and or the provision of train-the-trainer interventions.
2. Provide Technical training to IS&T resources to perform first-line support.

3. Provide input into change management activities and ensure Business Users are able to maintain productivity during the transition.
4. The vendor must provide a comprehensive implementation plan and initial on-site as well as long term second line remote support over the lifetime of the solution 365/24/7.
5. Reviewing and enhancement of applicable Document and record management procedures and processes.
6. Identification and input towards procedures and processes to be developed.
7. Review of the existing taxonomy, thesaurus, file classification systems and conversion to the new system.
8. Analysis of data and content and engaging business areas and key stakeholders to assist with developing classification schemes and confirming or identifying retention periods.
9. Reduce any document and records duplications that might exist in the current systems and resolve based on migration strategy guidelines to be developed with the successful vendor.
10. To provide an RM&DM&CM solution that fulfils the goals, objectives and functional requirements as stipulated in this document.

13.2.2 OUT OF SCOPE

The following are out of scope:

Out-if-scope consideration	Reasoning
Back scanning of existing paper-based documents	The existing contract is in place to perform back scanning. Any additional back scanning requirements should be treated as separation of tender and services interest to minimise any distraction from the tender provisions
Change Management – this would be managed by another 3rd party as part of the initiative.	Separate human-based intervention from technical tender considerations. The RM&DM&CM vendor/s will provide input into the change management intervention but will not be required to perform the actual change management interventions

Table 1: Out of scope items

13.3 CURRENT ARCHITECTURE AND LANDSCAPE

In the past few years, the City of Cape Town (CCT) has invested extensively in Microsoft SharePoint as a repository platform that has been customised as a document management solution as well as SAP RCM for the structured data element as well as case management. The file server, FS01, has been utilised as a storage location for specific technical file types that could not be catered for within SharePoint but has also become a repository for documents and records.

SAP RCM is the union of Records management and Case Management with some additional features focusing, specifically on the public sector. The goal of the SAP RCM is to manage business process-related documents following the public sector laws, rules, and practices. SAP RCM currently encompasses two environments, SAP Public Sector Records Management (SAP PSRM) and SAP ECC6 Records and Case. Reference to SAP RCM will include these two environments.

Since Records and Documents management is workflow centric, that can include some complex workflows, it is recommended that the Workflow component of the awarded solution is considered as a broader workflow solution for the City outside of just Records and Document Management, e.g., say for the HR system or the procurement processes.

Since local government procurement is a record and document-centric workflow process, it is proposed that this is implemented as a priority in the implementation phase.

It is critical to note that some of the technology is nearly 20 years old and the as-is documentation and process maps are not readily available because this enterprise IP are in the heads of a few old stall wards.

Other tenders that are currently been drafted that will impact the future IT software landscape focus on the provision of an ERP solution, Access Management, and the implementation of integration

software/solution/standards.

Whether Microsoft and SAP will be replaced or upgraded, or whether these solutions will be managed on-site or in the cloud, will have an impact on the workflow and integration points.

Current SharePoint and SAP landscape:
The diagram below provides a high-level overview of the current landscape:
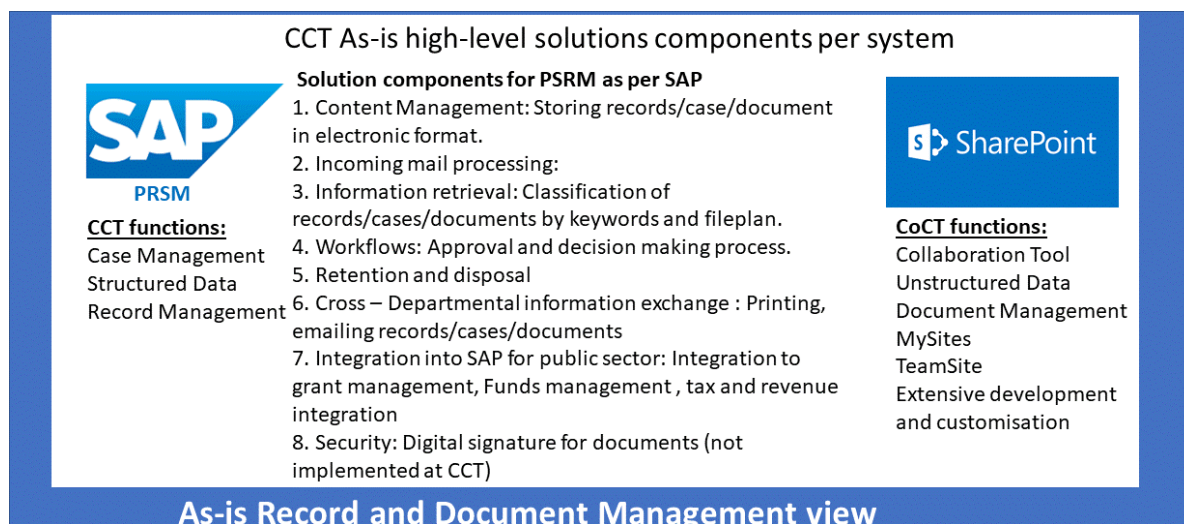

Figure 1: High level overview of current landscape
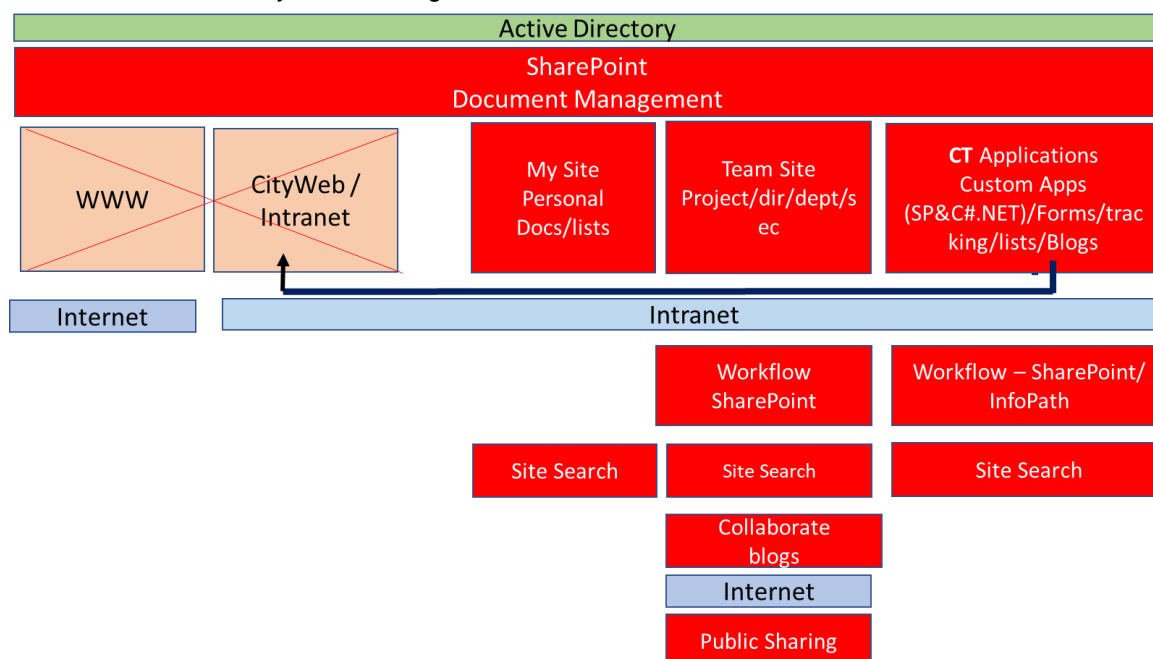
SharePoint:

SharePoint as-is eco system at a high level:

Figure 2: High level SharePoint eco system

- A typical SharePoint site contains the following components:
  - webpages,
  - document libraries,
  - lists,
  - a newsfeed,
  - and other apps.

- These items are linked together within the site structure

In addition to its own components, such as pages and document libraries, a SharePoint site can have many sub-sites, the hierarchy of which, on web servers, resembles the hierarchy of folders on file systems.

TeamSites:

A City TeamSite is a SharePoint site that provides Directorates/ Departments/Branches and Project Teams with the ability to share documents across the City. A TeamSite connects the user and their team to the content, information, and applications they rely on every day.

MySites:

A MySite is the user's personal site on Microsoft SharePoint. Each City staff member is provisioned with a City MySite that offers the same functionality as a TeamSite but has less storage space allocated.

CTApps:

CTApps are standalone applications that have been developed utilising the SharePoint platform to meet a specific business requirement.

- Although the SharePoint platform provides a number of features that can be utilised for various purposes, the table below represents the key functional items used in TeamSites, MySites and CTApps.
- It is important to note that departmental business owners have the ability to configure or request configuration of these items to meet a variety of business needs of varying complexity.

Item	Description	Available in
App Launcher	Access to pre-built apps that users can create and configure to meet their specific business needs e.g. document libraries, custom lists, tasks, announcements etc.	TeamSites, MySites, CTApps
Document Libraries	A Document Library is a place for storing various types of files that can be shared. To organise files, additional Libraries for documents, pictures, slides, etc. can be created.	TeamSites, MySites, CTApps
Lists	SharePoint lists can be created by using list templates, such as calendar and tasks, by importing spreadsheets, and by creating custom lists. Lists can include many kinds of data, ranging from text and dates, to calculations based on other columns.	TeamSites, MySites, CTApps
Web pages	Users of TeamSites and MySites have the ability to create and configure Web pages. This functionality also allows the users to include App parts and Web parts and all of its features in a Web page.	TeamSites, MySites, CTApps
Forms	Basic to highly customised forms have been built to capture information into a CTApp.	CTApps
Workflow	Basic to highly customised workflows have been built to cater for the approval of requests and applications specific to a business process or task.	CTApps
	Business users have the ability to utilise out of box workflows in MySites and TeamSites.	TeamSites, MySites

Table 2: Key components of SharePoint sites (not exhaustive list of all features)

- **Tools/Frameworks utilised**:
  - InfoPath for form building
  - SharePoint Designer for Out of the Box development and workflow building
  - JavaScript

- **Integrations**:
  - Certain CTApps are currently communicating with other applications in the CCT. This communication is via custom-built web services or data connections. The SharePoint List Web Service is the predominantly utilised method for these points of interaction. **Refer to Schedule 15I**

- **Custom built applications**
  - The CCT also has a variety of custom-built applications that have been developed utilising the .NET platform. Some of these applications are utilising SharePoint functionality in the form of lists and workflows and are closely integrated with CTApps.

The table below represents the scope and size of the current landscape as it pertains to the utilisation of SharePoint in the CCT. The .NET applications have also been included due to the utilisation of SharePoint functionality and integration with SharePoint applications. This table provides the scope of the sites and applications to be included in the implementation that specifically relate to SharePoint.

System	Type	Consists of	Volume	No. of Files	Workflows	Configure/ Develop	Migrate (Metadata and documents)	Integrations
Custom Dev (.NET)	Custom	• Lists and workflows • Documents and records	N/A	N/A	N/A	N/A	N/A	7
SharePoint	CTApps	• Out of the Box (OOTB) functionality • Custom with OOTB functionality • Lists with workflows • Forms with workflows • Web pages • Documents and records	Approx. 0.491TB	1 178 400	735	110	110	9
	MySites	• Lists • Images • Web pages • Documents and records	6.2TB	8 061 776	0	17 700	17 700	N/A
	TeamSites External TeamSites		36.1 TB	28 907 916	0	3200	3200	N/A

Table 3: Scope of SharePoint migration and implementation. The figures in the table above indicate current volumes and will be confirmed during implementation of the solution.

SAP RCM:

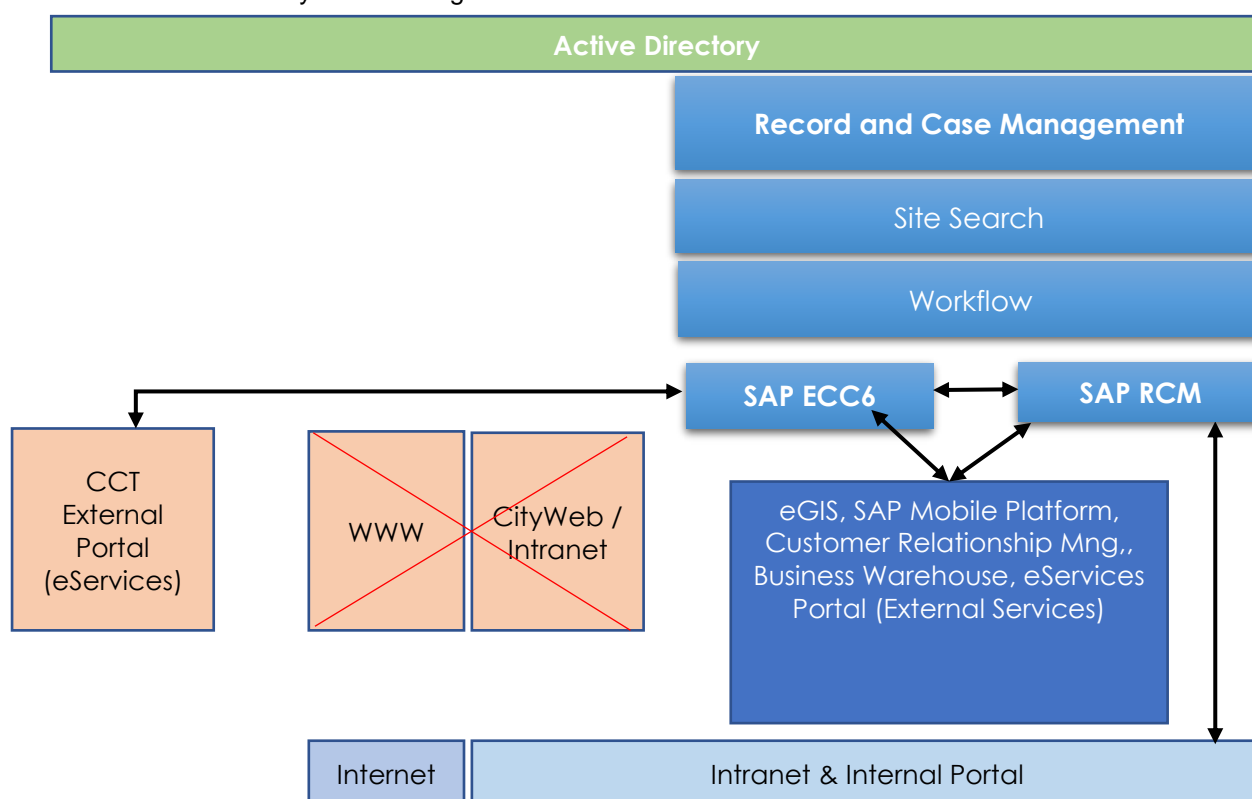SAP RCM as-is eco system at a high level:

Figure 3: SAP RCM high level eco system

- • The SAP RCM suite is comprised of two main components:
  - o SAP PSRM and ECC6 Records and Case are highly customised environments; both catering for records and case management functionality.
  - o Workflow packages are templates utilised to create workflows

It is envisaged that physical registries will be reduced as we evolve our digitisation processes and in future all the relevant artefacts and related data will have to be digitised and transferred to the new environment.

The CCT SAP footprint extends over 17 systems that integrates with each other across a single landscape. It is important to note that the SAP RCM System is the official Records Management system of the CCT. It has two main functional areas that are different in nature, but are still stored as records namely:
- • Records Management
- • Case Management
Records are stored across systems and modules therefore it is not always clear who the Business owners are for a record as the records may relate to more than one Business Process.
Records are being stored via three main methods within the CCT's classification systems:
  - o Upload of single document via the SAP Graphical User Interface (GUI)
  - o Bulk upload of documents via the SAP GUI
  - o Upload of documents via another SAP module/system utilising Generic Object Services (GOS)
The list below is an example of records created in SAP RCM and that are stored within the system:
- • Indemnities
- • Leases
- • Response Letter (CCT)
- • Incoming Correspondence (CCT)
- • Acknowledgement of debt
- • Contracts
- • Deeds

- General Agreements (e.g., MOU)
- Guarantees
- IT Contracts
- Banking Reply File
- Account Pay (AP) Invoices
- AP: Reconciliation Statements
- Sundry Invoices

The bulk of the operational records are being stored in the source systems.

- Integrations:
  - o The SAP RCM solution has multiple integrations with other SAP modules and systems as well as the CCTs' Enterprise Geographical Information System (EGIS). The integrations are predominantly built utilising the SAP Remote Call Function (RFC) method to handle the communication between systems.

Additional detail in the SAP ECC6 and RCM integration blocks can be further expanded to reveal the following integrations
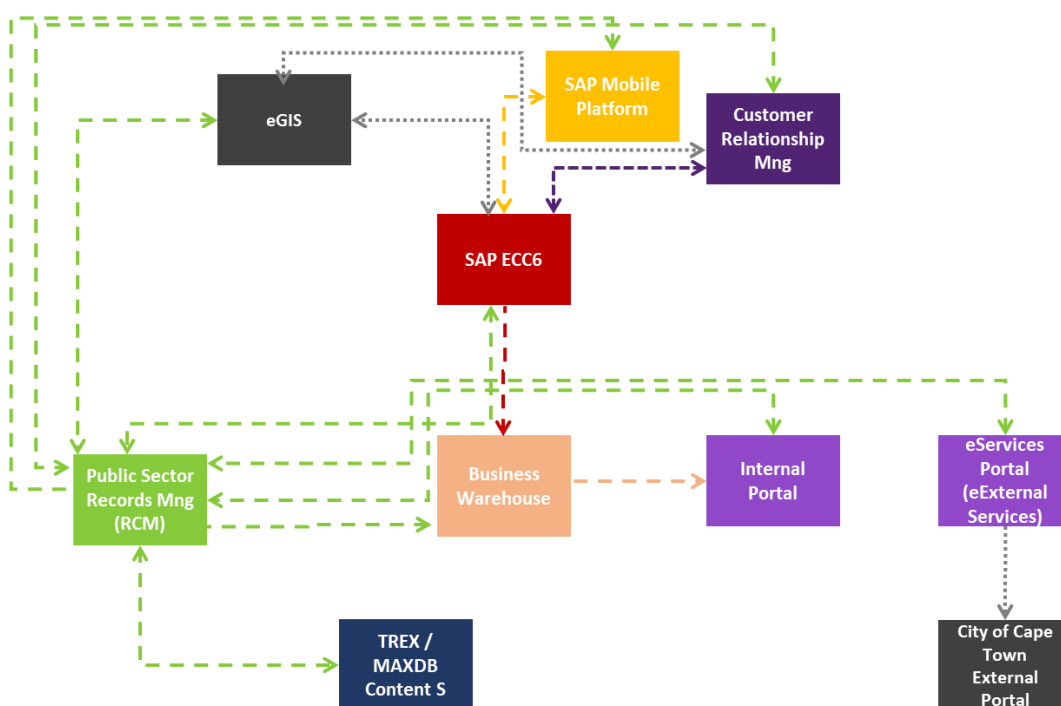

Figure 4: High SAP RCM integration

The table below represents the scope and size of the current landscape as it pertains to the utilisation of SAP RCM in the CCT. The GIS applications have also been included due to the integration with SAP RCM. This table provides the scope of the solutions and sub process to be included in the implementation that specifically relate to RCM.

System	Type	Consists of	Volume	No. of Files	Workflow Packages	Configure/ Develop	Migrate (Metadata and documents)	Integrations
SAP RCM	PSRM (NXP)	• OOTB functionality • Custom with OOTB functionality • Forms with workflows • Cases and workflows • Documents and records	Approx. 20TB	33 811 818	206	30 solutions 160 sub processes	30 solutions 160 sub processes	363
	ECC6 Records and Case (RP1)							
SAP ECC6 Documents	ECC6 Modules	• OOTB functionality • Custom with OOTB functionality • Forms with workflows • Cases and workflows Documents and records	Approx. ~40TB	To be identified during analysis	To be identified during analysis	To be identified during analysis	Approx. ~40TB	To be identified during analysis
ESRI	Spatial (EGIS)	N/A	N/A	N/A	N/A	N/A	N/A	2

Table 4: Scope of SAP RCM migration and implementation. The figures in the table above indicate current volumes and will be confirmed during implementation of the solution.

In addition to the SAP RCM volumes, SAP ECC6 contributes to approximately 40TB of documents that are required to be analysed, retention periods identified and classified in the RM&DM&CM solution. These documents are not currently linked to the classification systems but will be required to be classified as records in the RM&DM&CM solution.

File Server: FS01

FS01 is a windows server environment and is currently utilised as a repository for CCT employees doing their day-to-day activities, projects, development and storage of in-process data. It is the central file server utilised in the CCT for storing a number of various file types. The file server currently provisions storage space for the G and I drives and is utilised by business units across the CCT.

System	Type	Consists of	Volume	No. of Files	Configure/Develop	Migrate (Metadata and documents)	Integrate
File Server (FS01)	G: Drive	• GIS data and imagery • Audio and video • Databases and troubleshooting tools • Documents and records	Approx. 29.9TB	13 710 519	N/A	Approx. 29.9TB	N/A
	I: Drive	• Images and video	Approx. 11.8TB	1 337 755	N/A	Approx. 11.8TB	N/A

Table 5: Scope of FS01 migration and implementation. The figures in the table above indicate current volumes and will be confirmed during implementation of the solution.

13.3.1 Current SharePoint, SAP RCM and FS01 ISSUES

During the as-is assessment the following pain points, issues and system deficiencies were identified. Some of the issues are related to staff behaviour and will have to be changed via change management and or consequence management interactions.

Current issues in SharePoint
- Size limitations on file size and total storage.
- Folders created with no real structure.
- No corporate guidelines on version control, retention and disposal of content.
- No corporate guidance on classification of content.
- Limitations for multimedia files.
- No integration with SAP RCM - integration standards.
- Used as archival system.
- Numerous classification schemes exist.
- Lack of Governance (roles and responsibilities, accountability, Monitoring & Evaluation).
- Internet has become the repository for document management.
- Ownership of content from the internet e.g. "Who is governing the taxonomy?"
- Shared drives- unstructured data scattered across departments not incorporated and controlled via the current document management solution, namely SharePoint.
- Loss of system derived metadata in SharePoint requires additional metadata to be captured manually if the document converts to a record.

Current issues in SAP RCM
- No compatibility/integration into National Archives.
- Not aligned to any corporate classification scheme.
- In the SAP Records & Case Management, there are records stored that are not declared into the CCT classification system. These records are safely stored and can be easily retrieved when required via the process case it was created in.
- Records are stored across systems and modules therefore it is not always clear who the business owners are for a record as the records may relate to more than one business process.
- The bulk of the operational records are being stored in the source systems.

- Not all functionality currently utilised in the CCT

Current issues in FS01
- Lack of governance
- Lack of document management principles
- Various files types stored including from the more common file types such as pdfs to database files

13.3.2 CCT's CURRENT SAP AND MICROSOFT ENVIRONMENT

13.3.2.1 SERVER APPLICATIONS

Operating Systems

Technology	Status
Microsoft	MS Windows server 2012 R2 as the minimum standard
SAP	AIX 7.1 as the minimum standard
	SLES 11.4
FS01	MS Windows server 2012 R2 as the minimum standard

Database

Technology	Status
Microsoft	MS SQL 2015 as the minimum standard
SAP	Oracle 12.1 as the minimum standard
	SAP HANA SP12

Server Virtual Machine

Non-SAP Applications and databases are hosted in the Virtual Machine (VM) Servers

Technology	Status
Microsoft	Microsoft Hyper-V
SAP	Power VM

Server Management

Technology	Status
Microsoft	System Centre Suite 2012 (Configuration Manager, Operations Manager, Endpoint Protection and Virtual Machine Manager)
SAP	Solman 7.1

Backup and Recovery Software

Technology	Status
Microsoft	Veritas Netbackup 9.1 as the minimum standard
SAP	Veritas Netbackup 9.1 as the minimum standard

Authorization and Authentication

Technology	Status
Microsoft	Active Directory Services (Windows Server 2012)
SAP	SAP NetWeaver Authorisation

13.3.2.2 DESKTOP/WORKSTATION APPLICATIONS

Technology	Status
Microsoft	Windows 10 Pro v21H1 64-bit Enterprise and Windows 10 64 bit Professional and Enterprise as the minimum standard

Desktop Productivity Suite

Technology	Status
Microsoft	Office Professional Plus 2010 as the minimum standard {Word, Excel, PowerPoint, Outlook, OneNote, InfoPath reader (electronic forms client), Lync (corporate instant-messaging client), SharePoint }

Internet Browser Software

Technology	Status
Microsoft	Internet Explorer 11 as the minimum standard

Anti-Malware Software

Technology	Status
Microsoft	Trend Micro Apex One as the minimum standard

ERP Client Software

Technology	Status
SAP	SAP GUI 7.4 as the minimum standard

13.3.2.3 NETWORK

The City's network is spread over a wide geographical area which runs on a Multiprotocol Label Switching (MPLS) network.

Desktops typically have a 100Mbps LAN connection, while WAN connections vary between 28.8Kbps to 1Gbps (a typical WAN connection is 64Kbps).

Servers in the datacentres are linked to a minimum of 1 Gbps of connectivity.

13.3.2.4 DESKTOP HARDWARE

The City of Cape Town's minimum desktop hardware specification are:
o Processor: Intel® Core™ i5-4590
o Memory   4GB
o Chip Set   Q87 (Latest Intel AMT 9.0 with full *Intel® vPro™* manageability)
o Hard Drive: 320GB HDD
o Graphics   Intel: HD 4600
o Memory Slots: 2
o OS Windows 7 Enterprise Edition and Windows 10 Professional Edition

13.3.2.5: DEPARTEMANTAL USAGE OF SAP RCM

SAP RCM is currently utilised across departments in the CCT.

13.3.3   EIM/IIM or ECM or RM&DM&CM

The tender refers to Document and Record management and these functionalities are viewed as the heart of an ECM or EIM/IIM system.

The expressed need of the CCT is RM&DM&CM functionality. These functionalities can exist with an ECM or EIM/IIM solution but where the RM&DM&CM modules are only activated for now and the purchase and annual maintenance fees are not based on the complete ECM or EIM/IIM packages but only on the selected modules to fulfil the expressed functional and non-functional requirements as contained in this document as mandatory minimum requirements. The CCT must be able to activate other modules of the ECM or EIM/IIM solution if the future need arises.

13.3.3.1 RM&DM&CM ARTEFACT OVERVIEW

Below is a list of artefacts that currently exist. These might not be up to date and might have to be adjusted or optimised to ensure the implementation of an optimal solution. The CCT will rely on the expertise of the implementation vendors to advise and guide them during the implementation phase for these corrections to take place:

- Taxonomy- indication is that the current taxonomy can be utilised as-is. However, a review of the current taxonomy to ensure that it aligns with the currently accepted practices are recommended.
- Thesaurus -The current thesaurus is very rudiment and the utilisation of an internationally accepted thesaurus artefact might be considered with the approval of management as part of the system configuration process.
- Filing plan -The CCT's current file plan needs to be reviewed in the light of South African National Archives Directive R5: Prototype of File Plan for Local Government with National Archives or Provincial Archives as a potential additional external stakeholder for consideration.
- Records Management System and Procedure – The City's RM system and procedure was reviewed and approved by the Provincial Archives in 2021, now called RM System and Procedure. The RM System and Procedure includes a section on electronic records

management. This section will need to be improved in line with the implementation of the RM&DM&CM solution.

13.3.3.2 FUTURE STATE

As indicated earlier in the document, the purpose of the tender is to provide a Document and Records Management functionality that caters for all the record, document and case management needs of the CCT as well as for the provision of Digital Signatures, an advanced search engine and publishing module as per the CCT's business requirement.

The need to utilize the RM&DM&CM workflow function as an Enterprise solution to manage workflow functions with or between other 3rd party software has also been expressed as an explicit requirement.

13.3.3.2.1 Future Architecture and Future Landscape

This section provides an overview of the changing IT landscape and environment within which the RM&DM&CM solution will have to function. The possible replacement and or upgrade of various systems would mean that the initial deployment of the RM&DM&CM system would be subject to possible ongoing IT landscape changes for a few years. The tender response should incorporate this future reality as part of the submission and the ongoing integration configuration and enablement tasks must form part of this tender response and tender costing exercise.

As part of the future digital approach, an additional two streams are tasked with the preparation of tender documents that consider the possible replacement or upgrade of SAP as well as the MS productivity suite.

The outcome of these streams will not be known when this RM&DM&CM tender is published and this might impact the implementation of the future RM&DM&CM solution concerning the ERP integration and document file extensions. The uncertainty about the ERP tender outcome also impacts the possible future of the SAP RCM module and hence the requirement for the RM&DM&CM solution to incorporate the provision of Case Management as currently catered for in the SAP RCM module.

Other projects that form part of the digitisation initiative at the CCT includes the upgrade of the EGIS system in parallel to this project, as well as the updating or replacement of Active Directory (AD), access control, integration as well as authentication.

The RM&DM&CM solution must therefore be able to operate in a future loose coupling environment. The information provided in the document below provides the full scope and the technical requirements that inform the details of this tender:

13.3.3.3 GAPS AND IMPROVEMENT OPPORTUNITIES

13.3.3.3.1: CURRENT GAPS BETWEEN CURRENT AND FUTURE STATE

The table below provides a comparative view of the current versus the expected future state where

the new RM&DM&CM system would provide the solution to bridge the existing gap.

Current scenario	Future requirement
Two systems are utilised namely SharePoint and SAP RCM	An integrated system to perform all the functions
Sign-on and different front ends to access SharePoint and SAP RCM	A single sign-on and a single interface to access all types of artefacts
The CCT's current file plan needs to be reviewed in the light of South African National Archives Directive R5	File plan reviewed and aligned to the South African National Archives Directive R5
The CCT's Records Management System and Procedure, was reviewed and approved by the Provincial Archives in 2021, now called RM System and Procedure. The RM System and Procedure includes a section of electronic records management. This section will need to be improved in line with the implementation of the RM&DM&CM solution.	A Record Management System and Procedure is available that reflects all the changes to the taxonomy, thesaurus and new system operations.
Not all the physical documentation are saved within the Document management system. Some of these physical documents are lying on the desks of staff members.	All documentation need to be incorporated into the new system and the utilisation of digital form and centralised e-mail boxes should be used to "intercept" these artefacts and to correctly allocate the taxonomy automatically to these artefacts to ensure proper compliance and governance. The scanning equipment should be setup to enable this functionality.
The SAP RCM workflow facility is utilised to manage the document and record management workflow	Utilize the RM&DM&CM workflow function as an Enterprise wide solution to manage workflow functions with or between other 3rd party software has also been expressed as an explicit requirement, if possible.
Multiple duplicate records exist that have a storage and financial impact on the CCT.	With the conversion of the old artefact to the new system, these duplicates will be identified and eliminated, as per existing records management procedures and vetted before deletion, leading to substantial cost and storage savings.
Documents that are saved in shared folders TeamSites, MySites and SAP ECC do not form part of the current RM&DM&CM solution	All documentation needs to be incorporated, classified, retention periods assigned, managed and controlled in the new RM&DM&CM.

13.3.3.3.2 IMPROVEMENT OPPORTUNITIES

The following improvement opportunities were identified as part of the documentation analysis:

- The incorporation and enforcement of all documentation to be included in the new system to ensure full accountability and traceability is available when considering these artefacts.
- The creation of a Centralised Document Repository that can be searched via a single search facility.
- Ensure all metadata is recorded and managed with minimal human intervention.
- Classification systems are reviewed quarterly and submitted to the Provincial Archives and records services for approval. The CCT's current file plan needs to be reviewed in the light of South African National Archives Directive R5: Prototype of File Plan for Local Government with National Archives or Provincial Archives as a potential additional external stakeholder for input. CCT management to produce this artefact.
- The CCT's Records Management System and Procedure, was reviewed and approved by the Provincial Archives in 2021, now called RM System and Procedure. The RM System and Procedure includes a section of electronic records management. This section will need to be improved in line with the implementation of the RM&DM&CM solution.

- Alignment and co-operation with international recognised world leaders on the provision of Thesauri can accelerate and reduce the cost of providing a world-class thesaurus for the CCT.
- Provide the facility for internal shared folders for departments and project teams that are not operating within the current TeamSite or MySite needs to be addressed to ensure shared folders are incorporated within the new system. This might require amendments to the HR policies and procedures that will enforce the appropriate consequence management penalties for non-compliance.
- The implementation of digital signatures and authorisations to support the digital aspirations of the CCT.
- Eradication of duplicate records as part of the migration of the existing artefacts to the new system in line with current records management procedures.
- The identification and destruction of documents and records that are past their due date and correcting these non-compliance issues as per existing records management procedures and vetted before deletion.
- Analysis of data and content and engagement with business areas and key stakeholders to identify retention periods and classify records appropriately.
- The review and possible amendment of the current taxonomy, classification systems and thesaurus would need to be performed to ensure the new system solution is configured with optimised information before system configuration.

13.4 FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

13.4.1 FUNCTIONAL REQUIREMENTS

The system that is required and referred to in the tender description as an Record Management and Document Management solution refers to a software solution that provides, document management, case management, record management functionality as well as digital signatures, as endorsed by the National and Provincial Archives, that fulfil the functional requirements as defined below. The utilisation of the workflow engine as an Enterprise-wide workflow engine also forms part of this tender.

To ensure that no preconceived ideas or misinterpretations of the requirements are created when referring to solution terminology, the requirements below would refer to the "system" to describe the software solution and the term "objects" refer to cases, document as well as records.

This section addresses the *minimum set of mandatory* baseline functional requirements applicable to the RM&DM&CM solution for the CCT.

Please note that the functional requirements are non-conditional requirements and are stand-alone requirements independent of any other requirement in the Specifications. These requirements are generally phrased: 'The term must/should/may … [description of functional requirement]'.

13.4.1.1 REQUIREMENT LEVELS

Each requirement in this document has been allocated a requirement level. The description of each requirement uses the keywords, 'must', 'must not', 'should', 'should not' and 'may' to indicate the obligation levels. These terms reflect established usage in tender documentation.

Mandatory - This is a compulsory non-conditional requirement for any system intended to keep digital records. 'Mandatory' requirements are essential for the establishment of adequate recordkeeping functionality within all RM&DM&CM software. They are identified by the use of the term 'must' or 'must not'.

Required - This is a compulsory conditional requirement that applies only when the RM&DM&CM solution supports one or more specific non-conditional requirements. If the RM&DM&CM solution does not support a specified prerequisite non-conditional requirement, the 'Required' requirement will not apply. Required requirements are identified by the use of the prefix phrase 'Where the RM&DM&CM solution [supports or does not support a particular feature]', and the use of the term 'must' or 'must not'.

Desirable - This is an optional requirement for any system intended to keep digital records. These requirements are not considered essential for the establishment of adequate recordkeeping functionality within an RM&DM&CM solution and none of these requirements are listed in the functional requirements specification. 'Desirable' requirements generally represent best practice and exceed requirements for adequate recordkeeping functionality. The applicability of desirable requirements must be assessed on a case-by-case basis. Desirable requirements are identified by the use of the term 'should', 'should not' or 'may'. Desirable requirements identified by the use of the term 'should' or 'should not' are optional but are highly recommended. Where a Desirable requirement uses the word 'may', the requirement is considered entirely optional and its implementation is at the discretion of the CCT.

13.4.1.2 SUMMARY OF FUNCTIONS

The City of Cape Town requires a RM&DM&CM Solution to replace the current solution that must comply with National legislation, regulations as well as local and international standards that must fulfil the following Case, Document and Records management primary functions:
- Control
- Capture
- Access and security in line with POPIA
- Access and security in line with POPIA and CCT permissions for back end servers
- Disposal
- Searching and retrieval
- Metadata
- Compliance
- Storing Records
- Document management

13.4.2 CORE FUNCTIONAL REQUIREMENTS

These functional requirements definition is related to **SCHEDULE A** in section **(5) Price Schedule** of this tender document. Refer 2.2.1.1.6 of the Eligibility Criteria. Tenderers are to confirm compliance to Specification by indicating **Yes/No** on **Schedule 15G** of the tender. If No, tenderers must provide comments / mitigation in relevant column. The Bid Evaluation Committee will assess whether the mitigation/ solution provided conforms to the scope required.

Where cloud offerings are proposed, please complete cloud assessment criteria Table as specified in **Schedule 15R** of the tender. The information provided will not be used for evaluation purposes.

Core Functional Requirement Category	Core Functional Requirement
Records management, Case Management & Document Management The Content management system must allow for the integration of both physical record and document files, digital records, cases and documents to be organised so that they can be managed, found and understood.	It is implied that this incorporates: • Business classification scheme • Records and Document classification tools and • Folder Management • Case Management

13.4.2.1 RECORDS MANAGEMENT

Core Functional Requirement Category	Core Functional Requirement

Control *The Records Management System (RMS) must allow folders and records to be organised so that they can be managed, found and understood.*	**Business classification scheme**
	• The system should support the representation of a business classification scheme that reflects the business activity of an organisation.
	• Where the RMS supports a business classification scheme,
	   ○ it must be able to track the development and maintenance of the scheme over time and form part of the Enterprise Information Architecture.
	   ○ It must allow centralised management of the scheme by the RM System Administrator or other authorised user.
	   ○ it must allow the separate development and use of more than one scheme.
	   ○ it must allow the definition of levels and the allocation of unique identifiers for business functions, activities, and transactions.
	   ○ it should allow linkages between functions and activities to exist over time.
	   ○ it may allow the entry of text-based scope notes and other descriptive information attached to functions, activities, and transactions.
	   ○ it may allow the entry of start and end dates for functions, activities, and transactions.
	   ○ it may allow the entry of source citations or mandates attached to functions, activities, and transactions.
	   ○ it may allow the mapping of functions, activities, and transactions to organisational structures.
	   ○ it may allow links to one or more term in external schemes such as Keyword AAA: or the aka schema.
	   ○ it may be able to import from, or export or link to, other systems where there is a close relationship between functional entities (as defined within the business classification scheme) and the functionality of other systems.

Core Functional Requirement Category	Core Functional Requirement

	o it may allow the entry or import of recordkeeping requirements for function/activity sets and transactions or groups of transactions.
	o it should enable links to records management mechanisms within the system – e.g. records classification tools, access controls and disposal classes/authorities.
	    ▪ and the records management mechanisms within the system, it must warn a RM System Administrator when control mechanisms linked to the scheme are updated.
	    ▪ and the records management mechanisms within the system, it must meet the metadata requirements specified for function entities as per the ISO international acceptable Record and Document management Metadata Standard
	o it should be able to export that scheme for use in a receiving system, maintaining all structural links between functions, activities, and transactions.

	Records classification tools The RMS • must allow records to be classified in accordance with the organisation's records classification scheme. • must support close linkage and interaction between records classification tools and other record and document management processes such as capture, access and security, disposal, searching and retrieval, and reporting. • must support the definition of a records classification scheme, to organise digital folders and records. • must ensure that the hierarchical accumulation of term within the definition of a records classification scheme, results in a unique record category. • must allocate a unique identifier to each term defined within a records classification scheme. • must allow a RM System Administrator or any other authorised user to make global amendments to the definition of a records classification scheme in a single process. • should not limit the number of levels permitted at different points within the definition of a records classification scheme. • must restrict the definition and maintenance of records classification tools to a RM System Administrator or any other authorised user.
	Folder Management The RMS • must allow the addition of digital folders to the lowest levels of a defined records classification scheme, to organise aggregations of digital records. • must be able to ensure that every folder is allocated to a record category within the records classification scheme. • should not limit the number of folders that can be allocated to a record category or defined within the entire system. • must allow a RM System Administrator to configure the naming mechanisms for entities within the record plan. • must be able to enforce the use of a records classification tool for naming new entities in the record plan. • must be able to automatically record the date of creation of a folder, as folder metadata. • must allow the separate entry of the date on which a folder was opened, which may precede the folder's date of creation. • must allow a folder or group of folders, and their attached records, to be moved and reclassified within the system by a RM System Administrator or any other authorised user. • must ensure that records attached to a folder remain correctly allocated following the reclassification of a folder so that all structural links remain in place. • must allow the manual or automatic update of all folder and record metadata attributes that are determined by classification, following the reclassification of a folder.

Core Functional Requirement Category	Core Functional Requirement
	- must allow a RM System Administrator or any other authorised user to enter (as folder metadata) the reason for the reclassification of a folder or group of folders in one operation. - must retain a history of folder reclassification, including a folder's original location. - must allow a RM System Administrator or any other authorised user to close a folder, ensuring that no new records can be added to that folder (but noting the next requirement below). - must allow a RM System Administrator or any other authorised user to open a previously closed folder for the addition of records, and subsequently close the folder again. This will not automatically update the closure date retained in the folder metadata. The action is taken (i.e., the addition of records) must be recorded in the relevant audit trail. - must automatically record the closing date of a folder and be able to use this metadata to support other records management functions, such as disposal (see the disposal section). - must ensure that closed folders and their contents are still accessible for retrieval and viewing purposes. - must prevent the destruction or deletion of folders, records, and associated metadata at all times, except as specified in the Disposal section.
	Records Metadata The RMS - must be able to capture and maintain metadata relating to any business classification scheme or records classification tools it supports, in accordance with the ISO Recordkeeping Metadata Standards and other relevant standards. - must prevent the unauthorised addition or amendment of metadata relating to a business classification scheme or records classification tools. - must enable lower levels in a defined records classification scheme hierarchy to inherit metadata from higher levels, at the time of creation. - should enable lower levels in a defined records classification scheme hierarchy to inherit metadata retrospectively, following a change to the metadata at a higher level. - must support the ability to amend or override inherited metadata by an authorised user. - must maintain a record of changes made to the business classification scheme or records classification tools over time. - must be able to capture and maintain folder metadata in accordance with the ISO Recordkeeping Metadata Standard for Commonwealth Agencies and other relevant standards. - The RMS must prevent the unauthorised addition or amendment of folder metadata elements. - must enable folders to inherit metadata from the records classification scheme at the time of the creation of the folders. - should enable folders to inherit metadata retrospectively, following a change to the records classification scheme. - must support the ability of an authorised user to amend or override metadata inherited by folders. - must allow user-defined metadata fields for the entry of descriptive information about the folder. - must closely link folder metadata to the functionality it represents. Folder metadata must provide both descriptive information and active support for achieving that functionality automatically.
Capture *The system must formally capture records regardless of their technical characteristics.*	**Record capture** The RMS - must ensure that digital objects can be captured, regardless of format and technical characteristics, so that they can be registered and stored as digital records. - must allow users to capture, register and store all digital objects in their native format. - must be able to capture a digital object even if the generating application is not present.

Core Functional Requirement Category	Core Functional Requirement
	- must not limit the number of records that can be allocated to a folder or captured within the entire system. - must be able to capture incoming and outgoing electronic messages and attachments: - as an automated process; and/or - as selected and directed by a user. - must be able to capture attachments and embedded objects together with electronic messages as either linked records or a single compound record. - must allow electronic messages and attachments to be captured from within an electronic messaging system, such as an email client. - must allow a user to choose whether to capture an electronic message, such as an email, with attachments as: - an electronic message only; - an electronic message with attachments; - the attachments only; - any combination of the above. - must be able to indicate whether an electronic message in the system has an attachment. - must be able to undertake the bulk capture of electronic messages relating to the same transaction. - must be able to capture a dynamic document, such as a dynamic web page, as: - a single compound record; - an aggregation of linked component records; - a snapshot – 'frozen' in time; - a collection of components that can be regenerated upon request; or - a combination of the above - must support the capture of digital records from a range of records generating systems. These may include: - common office packages; - workflow applications; - electronic messaging systems; - e-commerce and web transactions; - imaging and graphic design systems; - barcode support systems; - scanning applications - library management systems; - corporate systems; - business information systems; - security administration systems; and - multimedia applications. - must provide an application programming interface (API) to support integration with other business information systems, to enable the capture and processing of records of transactions in real-time. **Bulk Record Imports** The RMS - must be able to undertake a bulk import of records exported from other records management or document management systems, capturing: - digital records in their existing format, maintaining their content and structure; - digital records and their metadata, maintaining the relationships between them; and - the folder structure to which the records are assigned and associated metadata maintaining the relationships between them. - must be able to perform a direct bulk import of digital records with associated metadata that is presented in accordance with the Record and Document Management Metadata Standard mapping this to the receiving structures.

Core Functional Requirement Category	Core Functional Requirement
	Record types The RMS ▪ must support the definition of different record types as defined by a RM System Administrator, ▪ must be able to manage record types centrally, (in a Centralised repository) restricting their use to groups of authorised users, ▪ allow defined record types to behave differently, according to their specified metadata profile and management policy and must support a default record type, which is available to all users with the ability to create records, provided within the system or as defined by the RM System Administrator.
	Registration The RMS • must facilitate the registration process of records, in the case of a digital object, it must be marked as a formal record and registered into the corporate recordkeeping system. • must prevent any unauthorised amendment to the content of a registered digital record and must also always prevent the destruction or deletion of registered digital records and associated metadata, except as specified in the disposal section. Each registered record must have a viewable registry entry including associated metadata. • must be able to restrict the ability to amend the name of a registered digital record, • it must allow records and documents to be classified following the organisation's records and documents classification scheme at the time of registration. • must also prevent the storage of duplicate records. • shall provide a capability for referencing or linking and associating supporting and related records and related info such as notes, marginalia, attachments, and electronic mail-return receipts, etc., to a specified record. • must allow only authorized individuals to change or delete links and associations. • must provide the capability to link original superseded records to their successor records. • shall provide the capability to support multiple renditions of a record. These shall be associated and linked. • shall provide the capability to increment versions of records when filing. The system shall associate and link the versions. • shall link the record metadata to the record so that it can be accessed for display, export, etc. • shall provide the capability for only authorized individuals to modify the metadata of stored records. However, the system shall not allow the editing of metadata fields that have been specifically identified in the regulations as not editable. • The system shall enforce data integrity, referential integrity, and relational integrity.

	Filing Electronic Mail Messages (E-mail)
	The RMS
	• shall treat e-mail messages the same as any other record, and these shall be subject to all requirements of a record.
	• shall capture and automatically store the transmission and receipt data identified below if available from the e-mail system, as part of the record metadata when an e-mail message is filed as a record. The system shall provide the capability for editing
	
	    o Subject or Title,
	    o Author or Originator,
	    o Addressee(s), and
	    o the Other Addressee(s) metadata fields before filing. All other fields shall not be editable.
	• The Transmission and Receipt Data that must be capture includes:
	    o The intelligent name of the sender. The intelligent name refers to the birth name of the sender.
	    o The intelligent name of all primary addressees (or distribution lists).
	    o The intelligent name of all other addressees (or distribution lists).
	    o The date and time the message was sent.

Core Functional Requirement Category	Core Functional Requirement
	- o For messages received, the date and time the message was received (if available). - o The subject of the message. - The system shall provide the user with the option of filing e-mail and all its attachment(s) as a single record, or filing selected e-mail item(s) as an individual record(s), or to do both. When the attachment(s) is (are) filed as an individual record(s), the user shall be provided with the capability to enter the required metadata.
	Record movement The RMS - must allow the re-assignment of records from one folder to another by a RM System Administrator or an authorised user and must be able to automatically capture metadata acquired directly from an authoring application, an operating system, or generated by the system itself. - must also capture electronic message transmission data such as e-mails and map it to record metadata elements. - must generate an alert when records are changed deleted moved copied etc.
Access and security *The system must have the ability to assign rights and restrictions on the use or management of particular records to facilitate security and access control and integrate with the IS&T user access system*	**System access** The RMS - must allow for different roles to be created and assigned i.e. technical administration and business administration - must allow a RM System Administrator to set security parameters for failed login attempts and align these to the IS&T Directory Service Desk Authentication. - must provide a single sign-on screen that would provide access to the user for document management, record management, case management and GRC documents based on the user access rights. - must support a mechanism for managing access and security controls centrally that may be applied to users, documents, cases and digital records and other entities in the record plan. The access control also refers to the deletion or making existing user access groups inactive, effectively barring any access previously allowed by the group(s) as per the CCT's access control policy. **User profile Management** The RMS - must require a RM System Administrator to make users known to the system employing pre-defined user profiles, supporting valid authentication and the allocation of access and security controls, must allow (but not require) a RM System Administrator to allocate users to one or more pre-defined user access groups. - must ensure that all users are allocated one (or more) roles, and allow access only to system functions permitted by the role(s). based on the access and security controls linked to a role and inherited by users.
	File Classification systems - The RMS shall provide the capability for only authorized individuals to create, edit, and delete file plan components and their identifiers. The file plan components should be organized into logical sets that, when populated, will provide all the file plan references necessary to properly annotate (file) a record. - The system shall provide the capability for only authorized individuals to create, edit, and delete record folder components and their identifiers. Each component identifier shall be linked to its associated component and its higher-level file plan component identifier(s). - The system shall provide the capability to sort, view, save, and print user-selected portions of the file plan, including record folders.
	Access and security metadata - The system must support the progressive addition of metadata to documents and digital records and folders to support access and security as per ISO standards for Record and Document Management Metadata. - The system should be able to retain the details and date of amendments to access and security controls, as historical metadata for a user profile, digital record, folder, or other record plan entity.

Core Functional Requirement Category	Core Functional Requirement
	• The system must support the progressive addition of metadata to documents and digital records and folders to support privacy, freedom and protection of information and archives legislation as and when these are published.

	Access and security application
	The RMS must
	• allow each user to allocate to records and folders the same access and security controls contained in the user's profile.
	• prevent users from allocating access and security controls that are not contained in the user's profile.
	• support the allocation of all forms of access and security controls to digital records, folders and other record plan entities, including:
	    o predefined user access groups (a discrete list of named users);
	    o one or more individual usernames (an ad hoc list of named users); and
	    o security categories (only one category may be allocated per entity)."
	• allow any and all combinations of access and security controls to be allocated to digital records, folders and other record plan entities.
	• allow the update and amendment of the access and security controls on digital records, folders, and other record plan entities.
	• restrict access to digital records, folders and other record plan entities that have been allocated a predefined user access group, to those users who are members of that group.
	• restrict access to digital records, folders and other record plan entities that have been allocated multiple predefined user access groups, to those users who are members of those groups.
	• limit access to digital records, folders and other record plan entities that have been allocated one or more individual usernames, only to those users so named.
	• allow all users (unless restricted by user role) access to all digital records, folders and other record plan entities which are not allocated any access or security controls.
	• restrict access to digital records, folders and other record plan entities, to those users or groups who have been allocated an equivalent or higher security category.
	• ensure that digital records and folders automatically inherit access and security controls from higher levels of the record plan under which they are created.
	• allow inherited access and security controls to be overridden by an authorised user, in accordance with the organisation's security model.
	• be able to automatically upgrade the security category of a digital record or folder, in accordance with the organisation's security model.
	• require the allocation of a single security category to a digital record, folder or other record plan entity, with the default being the lowest category.
	
	• restrict access to digital records, folders and other record plan entities which have been allocated one or more forms of access and security controls, only to those users who have been allocated all equivalent controls – and prevent access by users who have been allocated some, but not all, equivalent controls.

	Access and security metadata
	The RMS must
	• support the progressive addition of metadata to digital records and folders to support access and security as set out in the Record and Document Management Metadata standards
	• support the progressive addition of metadata to digital records and folders to support privacy, freedom of information and archives legislation, including:
	    o information about the release of digital records and folders, which may be used to retrieve details from another system;
	    o disclosability and exemption indicators; and
	    o full details of record creation, modification and preservation to assist in determining the age of long-term records,

Core Functional Requirement Category	Core Functional Requirement
	Extraction • The system must allow the creation of an extract from a digital record, whereby sensitive information is removed or hidden from view in the extract, while the originating record remains intact, as well as provide solutions for expunging sensitive information from all record forms it can capture, including audio and video. • The system must note the creation of an extract in the metadata of the originating digital record, including date, time, creator and reason for the creation of the extract as well as be able to copy metadata attributes from the originating digital record to an extract – allowing selected elements to be amended as necessary.
	Preserve records. The system should enable the organization to support the following capabilities in compliance with the records management policy(ies): • ensure that all records can be read and accurately interpreted throughout their useful life in that system; • enable migration of records to new storage media or formats to avoid loss due to media decay or technology obsolescence; • ensure that all captured metadata remains linked to appropriate records and is unchanged throughout the useful life of the records, including after migration to new media or technology; • monitor storage capacity and utilization, and alert system operators when action is needed (e.g., to increase capacity, back-up system files).

	Audit trail
	• The system must be able to automatically record information in the audit trail about the following events:
	    ○ creation of a new user or group;
	    ○ date and time of registration of all records;
	    ○ changes to access and security controls affecting a record, folder or user;
	    ○ relocation of records to another folder, identifying both origin and destination;
	    ○ relocation of a folder to a different part of the record plan, identifying both origin and destination;
	    ○ date and time of a change made to metadata associated with folders or records;
	    ○ all disposal review decisions made by a RM System Administrator;
	    ○ reapplication of a disposal authority to an entity, identifying both previous and subsequent authorities.
	    ○ placing or removing a disposal freeze on a record or folder, and
	    ○ a separate log of all deletion or destruction actions carried out by any user.
	    ○ Create and maintain an audit trail (also called use-history metadata) for all records activity and system functions.
	    ○ Provide access to audit trail information in the fullest detail (e.g. each individual record access,
	    ○ including record identifier, time, date, and user).
	• Provide summary reports of audit trail information (e.g. number of accesses).
	• The track failed attempts of all records activity and system functions.
	• Maintain audit trail information (e.g., number of accesses, details of individual record retrievals, attempts to delete a record) so that it can be managed as a record.

Disposal *The RMS must be able to control the retention and disposal of records held by the the system, in accordance with*	**Disposal** • The system must be able to control the retention and disposal of objects held by the system (electronically or physically), in accordance with disposal authorisation regulations and guidelines whether WCARS or NARSSA. • The system should provide managed information storage and access as well as legal hold capabilities to ensure the preservation of information.

Core Functional Requirement Category	Core Functional Requirement

disposal authorisation.	**Disposal authorities**
	• The system must support the controlled disposal of records legally authorised for disposal, either following approved disposal authorities issued by the Western Cape (WC) Provincial Archives or under a specific legislative requirement for the disposal of particular records.
	• The system must support the definition and application of the following disposal actions:
	o review;
	o export;
	o transfer; and
	o destruction.
	• The system must be able to import and export a set of disposal classes in a standard format defined by the WC Provincial Archives.
	• The system must allow a unique identifier to be assigned to each disposal class and, where applicable, must allow the disposal class to be associated with the appropriate disposal authority.
	• The system must be able to maintain a history of all changes to disposal classes, including date of change and reason for change as well as restrict the ability to create, edit and delete disposal classes and disposal authorities to the RM System Administrator or other authorised user.
	• The system must ensure each disposal class consists of:
	    o a disposal trigger, to initiate the retention period;
	    o a retention period, to establish how long the record must be maintained; and
	    o a disposal action, to prescribe the fate of the record.
	• The system must allow retention periods to be defined from one day to an indefinite length of time and ensure that any amendments to a disposal class take immediate effect on all objects to which that class has been applied.

Core Functional Requirement Category	Core Functional Requirement

	Disposal application
	• The system must allow disposal classes to be systematically applied to documents, digital records, folders and other record plan entities where supported.
	• The system must allow a disposal class to be applied at any level in the record plan, and inherited by descendant objects as they are created as well as enable the manual update or retrospective inheritance of disposal classes when a new disposal class is applied at a higher level of the record plan.
	• All disposal actions must be recorded in an audit trail
	• The system must support a disposal process consisting of:
	   ○ automatic identification of documents and digital records and folders for which the retention period has elapsed;
	   ○ execution of the relevant disposal actions after confirmation by a RM System Administrator or other authorised user.
	• Where the system supports folders, it must ensure that any disposal action applied at folder level is carried out on the complete folder contents.
	• The system must ensure that a retention period is calculated in real-time and cannot be artificially advanced and it must support external disposal triggers based on a notification of a defined event as entered by a user.
	• The system must automatically seek confirmation from a RM System Administrator or any other authorised user before implementing any disposal action and notify the RM System Administrator regularly of all disposal actions due to occur in a specified pre-defined period.
	• The system must allow a disposal freeze to be placed on a document, digital record, folder or other record plan entity, to prevent any disposal action from taking place for the duration of the freeze and prevent the deletion of any object subject to a disposal freeze.
	• The system must be able to identify any conflict between disposal actions and either:
	   ○ automatically apply the correct disposal action according to precedence defined by the organisation; or
	   ○ notify the RM System Administrator or any other authorised user and request remedial action.
	• The system must generate a certificate for records which have been disposed

	Scheduling Records.
	• The system shall provide the capability for only authorized individuals to view, create, edit, and delete disposition schedule components of record categories.
	• The system shall provide the capability for defining multiple phases (e.g., transfer to inactive on-site storage, transfer to off-site storage) within a disposition schedule.
	• The system shall provide the capability for only authorized individuals to define the cut-off criteria and, for each life cycle phase, the following disposition components for a record category:
	   ○ Retention Period (e.g., fiscal year).
	   ○ Disposition Action (interim transfer, accession, permanent, or destroy).
	   ○ Interim Transfer or Accession Location (if applicable).
	• The system shall, as a minimum, be capable of scheduling and rescheduling each of the following three types of cut-off and disposition instructions:
	   ○ *Time Dispositions*, where records are eligible for disposition immediately after the conclusion of a fixed period of time following user-defined cut-off (e.g., days, months, years).
	   ○ *Event Dispositions*, where records are eligible for disposition immediately after a specified event takes place (i.e., the event acts as cut-off and there is no retention period).
	   ○ *Time-Event Dispositions*, where the timed retention periods are triggered after a specified event takes place (i.e., the event makes the record folder eligible for closing and/or cut-off and there is a retention period).
	• The system shall provide the capability to automatically calculate the complete life cycle, including intermediate phases, of record folders and records not in folders.

Core Functional Requirement Category	Core Functional Requirement
	• The system shall provide the capability for rescheduling dispositions of record folders and/or records (those not in folders) during any phase of their life cycle if an authorized individual changes the disposition instructions. This requirement includes the capability to change the cut-off criteria of disposition instructions and to change the retention period associated with a disposition. • The system shall provide recalculation of the record life cycle based on changes to any life-cycle date and set the filing status (i.e., open, closed) of the folder according to the business rules associated with date change(s).

	Review
	 • The system must make all metadata relating to a digital record or folder under review available to the reviewer and must make the entire contents of a document or digital record or folder under review available to the reviewer, subject to applicable access restrictions. The applicable disposal class details must also be available to the reviewer either by searching or navigation.
	 • When a review disposal action is triggered, the system must allow the RM System Administrator to reapply a disposal class which could:
	    o mark digital records and folders for further retention and later review;
	    o mark digital records and folders for immediate export, transfer, preservation treatment (through a technique such as migration) or destruction; or
	    o mark digital records and folders for further retention and later export, transfer, preservation treatment (through a technique such as migration) or destruction.

	Export and transfer
	 • The system must be able to export digital documents and records, folders or other record plan entities, and all associated metadata to:
	    o another system within the organisation;
	    o a system in a different organisation; or
	    o the Western Cape Provincial Archives for the long-term preservation of digital records or documents appraised as having archival value.
	 • The system must ensure that any export action can include:
	    o all digital objects and folders that qualify for export under a disposal class;
	    o all metadata associated with exported digital objects, folders and other record plan entities; and
	    o all audit trail data associated with exported digital objects.
	 • The system must be able to export groups of digital records or folders in one sequence of operations such that:
	    o the content and structure of digital records and folders are not degraded or corrupted.
	    o all components of a digital record or document are exported as one unit;
	    o associations are retained between exported objects and their metadata; and
	    o relationships are maintained between exported objects so that their structural links can be re-built in the receiving system.
	 • The system must be able to export all the types of records it can capture, regardless of format or the presence of the generating application and must be able to export digital objects in their native format (or the current format to which they have been migrated).
	 • The system must allow digital objects to be exported more than once and
	 • must support a two-stage transfer process, consisting of:
	    o export of all digital records and folders that qualify for transfer under a disposal class; and
	    o destruction of the exported digital records and folders following confirmation of successful export.

	Destruction • The system must ensure that destruction results in the complete obliteration or inaccessibility of all objects as authorised, that they cannot be restored through operating system features or specialist data recovery techniques. • The system must prevent the destruction of digital records and documents or folders until a confirmation is received, and allow the process to be cancelled if confirmation is not received that will lead to all alternative renditions of that record are also destroyed.

Core Functional Requirement Category	Core Functional Requirement
	• The system must distinguish between an ad hoc delete function and the destruction function within the disposal process so that each can be allocated individually to authorised users. • The system must prevent the delete function from being used within the disposal process so that immediate destruction can only be achieved through the allocation of a disposal class.
	Disposal metadata • The system must support the progressive addition of metadata to digital documents and records and folders to support disposal and must be able to export metadata in an XML format as set out in the Record and Document Management Metadata standards. • The system must be able to record the date and details of all disposal actions as a folder and/or record metadata.
Searching and retrieval *The system must be able to retrieve digital records and folders by a variety of search methods, and render the results on-screen.*	**Search** • The system must provide search facilities to meet the needs of a range of users, from casual to sophisticated and must support the input of user-defined parameters to locate, access, retrieve and view records, folders and other record plan entities, and associated metadata. • The system must be able to withhold all or part of a search result, according to access and security controls as specified in the "Access and security" specification above. • The system must support the construction of searches by combining multiple terms from multiple sources. • The system must support the configuration of default search options for end-users as well as support the definition, saving and re-use of searches by end-users.
	Retrieval • The system must be able to retrieve digital objects, documents or records and folders by all implemented naming principles as well as by their associated unique identifiers. • The system must be able to retrieve a complete folder and all its digital records and contextual metadata and list all and only those records in the context of that folder as a discrete group and a single retrieval process. • The system must be able to retrieve and list a set of digital objects, taken from many different folders, where the record metadata or content meets the search criteria, and it must also support the simultaneous retrieval of digital objects, folders and metadata by multiple users. • When the system is updated the URL link allocated to an artefact then the UTL or nickname must remain with the artefact to ensure that the document can easily be retrieved even in the future in a new location.
	Display • The system must be able to display the content of all the types of digital records which it can capture, in a manner that presents all components of the digital document or record together as a unit in a manner that renders their original visual presentation and layout, without needing to load the generating application. • The system must be able to display all available metadata associated with a digital record or folder upon request. • The system should support the presentation or publication of digital objects, folders and associated metadata to a destination outside the system.
	Printing • The system must be able to print all the types of digital objects it can capture, without the use of 'screen dumps' as it might be returned by a search query or all the digital records in a folder to be printed in one operation. • The system must enable the printing of metadata associated with digital records and folders, including the ability to print barcode labels.

Core Functional Requirement Category	Core Functional Requirement
	• The system must include features for the suitable output of digital records that cannot be printed.
Metadata *The system must support the use of metadata to describe digital records, and to enable automated records processes.*	**Metadata configuration** • The system must support the range of metadata elements detailed in the Recordkeeping Metadata Standard as required by NARSSA and any other elements required to support the organisation's business and must be able to draw together all elements of metadata to create a metadata profile for a digital object, folder or other record plan entity where supported. • The system must place no practical limitation on the number of metadata elements allowed for each object in the system and must allow the RM System Administrator to specify which metadata elements are to be entered and maintained by keyboard entry or by drop-down list. • The system shall provide the capability for authorized individuals to designate the metadata fields that are to be constrained to selection lists and shall further provide the capability for authorized individuals to create and maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data. • The system shall provide the capability to allow only an authorized individual to define and attach user-defined business rules and/or access logic to any metadata field including user-defined fields.

Compliance
The system must meet relevant local, national, and international requirements for record management
	Legislation
	• Consideration for the Protection of Personal Information Act promulgated in 2019 and effective in 2020, and the Promotion of Access to Information Act with input from City Legal as a stakeholder
	• The system must support compliance with the recordkeeping, evidential, privacy and access provisions of all relevant South African legislation and regulations, including and not limited the to the following:
	    ○ National Archives Act and Record Service of South Africa Act No 43 of 1996 (as amended Act No 36 of 2001);
	    ○ Records Management Policy Manual National Archives and Records Service of South Africa, 2007;
	    ○ Western Cape Provincial Archives and Records Services Act
	    ○ National Records Management Policy. Records Management Policy Manual. National Archives and Records Service of South Africa, 2007;
	    ○ Managing Electronic Records in Governmental Bodies: Policy, Principles and Requirements (2006);
	    ○ Managing Electronic Records in Governmental Bodies: Metadata Requirements (2006);
	    ○ Policy Framework for the Government-wide Monitoring and Evaluation Policy System 2007;
	    ○ Minimum Information Security Standards of 1996 (MISS);
	    ○ Minimum Interoperability Standards (MIOS) for Information Systems in Government;
	    ○ Promotion of Administrative Justice Act (PAJA) 2000 (Act 3 of 2000);
	    ○ Promotion of Access to Information Act (PAIA) 2000 (Act 2 of 2000);
	    ○ Protection of Personal Information Act (POPI) 2013 (Act 4 of 2013);
	    ○ Electronic Communications and Transactions Act (ECT) 2002 (Act 25 of 2002);
	    ○ Public Finance Management Act 1999 (Act 1 of 1999);
	    ○ Municipal Finance Management Act No. 56 of 2003 (MFMA);
	    ○ Law of Evidence Amendment Act 1988 (Act 45 of 1988);
	    ○ Companies Act;
	    ○ Financial Intelligence Centre Act;
	    ○ Financial Advisory and Intermediary Services Act;
	    ○ The Income Tax Act;

Core Functional Requirement Category	Core Functional Requirement
	- VAT Act; - Customs and Excise; - Stamp Duties Act; - Prescription Act; - Insolvency Act; - King IV Code.

Standards

- Updates to ISO/DIS/SANS 16175: Information and documentation - Processes and functional requirements for software for managing records and to Relationship between the ISO/SANS 16175 series of standards and other products of ISO/TC46/SCII: Archives/Records Management
- The system should support compliance with all applicable South African and international standards. The standards do not replace the requirements contained in the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) (NARSSA Act) but affirm and support the statutory requirements.
- NARSSA endorses the standards listed below in so far as they serve as benchmarking tools for sound records management in governmental bodies and guide governmental bodies regarding other archival matters.
- Some, and not all, of the applicable standards are listed below:
    - ISO (SANS) 15489:2016 – Information and documentation – Records Management Part 1 and 2;
    - ISO (SANS) 15801:2017 – Document management - Information stored electronically - Recommendations for trustworthiness and reliability;
    - ISO (SANS) 30300:2020 – Information and documentation – Records Management – Core Concepts and Vocabulary;
    - ISO (SANS) 30301:2011 – Information and documentation – Management Systems for Records – Requirements;
    - ISO (SANS) 30302:2015 – Information and documentation – Management Systems for Records – Guidelines for Implementation;
    - ISO (SANS) 23081-1:2017 - Information and documentation - Records management processes - Metadata for records Part 1: Principles;
    - ISO (SANS) 23081-2:2009 - Information and documentation – Managing metadata for records Part 2: Conceptual and implementation issues;
    - ISO (SANS) 1828:2014 – Information and Documentation – Risk Assessment for Records Processes and Systems;
    - ISO (SANS) 18492:2005 Long-term Preservation of Electronic Document-Based Information;
    - ISO (SANS) 17799:2005 – Information Technology Security techniques – code of practice for information security management;
    - ISO (SANS) 14721:2012 – The Open Archival Information System (OAIS) Reference Model: Introductory Guide;
    - ISO (SANS)19005-1:2005 - Document management - Electronic document file format for long-term preservation Part 1: Use of PDF 1.4 (PDF/A-1);
    - SANS 19005-2:2011 - Document management - Electronic document file format for long-term preservation Part 2: Use of ISO 32000-1 (PDF/A-2);
    - SANS 16175-1:2014 - Information and documentation - Principles and functional requirements for records in electronic office environments - Part 1: Overview and statement of principles (Based on ICA-Req Module 1);
    - SANS 16175-2:2014 - Information and documentation - Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems (Based on ICA-Req Module 2);
    - ISO (SANS) 16175-3:2014 - Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 3:

Core Functional Requirement Category	Core Functional Requirement
	Guidelines and functional requirements for records in business systems (Based on ICA-Req Module 3); o ISO/TR (SANS) 13028:2010 - Information and documentation - Implementation guidelines for the digitization of records; o ISO (SANS) 25964:2011 - Thesauri and interoperability with other vocabularies – Part 1 Thesauri for information retrieval; o ISO (SANS) 25964:2013 - Thesauri and interoperability with other vocabularies – Part 2 Interoperability with other vocabularies.
	Guidelines • Consideration should also be given to the CCT's policies as well as the policies and protocols as specified by the Western Cape Government's WCARS (Western Cape Archives and Records Service). • The system should support best practice following all applicable NARSSA guidelines, including all other relevant guidelines where relevant. • The list below contains some of the guidelines that the system needs to adhere too and enforce: o The DOD 5015.2-Standard; o CCT Records Management System and Procedure; o CCT Information Security SOP; o CCT Electronic Communication SOP; o CCT Electronic Mail Usage Rules; o CCT IT Continuity SOP o CCT Business Continuity SOP; o CCT Data Strategy; o WCARS Digital Preservation Policy; o WCARS Naming Convention Protocol; o WCARS Digitalization Policy.
Storing Records The RMS must store records in a repository and these records must be accessed and managed through integration	• The system shall provide at least one portal that provides access to all associated repositories and databases storing electronic records and their metadata. • The system shall prevent unauthorized access to the repository (ies). • The system shall manage and preserve any record in any supported repository, regardless of its format or structure, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original. • The system shall allow only authorized individuals to move or delete records from the repository.

13.4.2.2 DOCUMENT MANAGEMENT

The Electronic Document Management (EDM) module must be able to provide or integrate with, document management facilities to ensure records management functions are seamlessly supported.

These functional requirements definition is related to **SCHEDULE A** in section **(5) Price Schedule** of this tender document. Refer 2.2.1.1.6 of the Eligibility Criteria. Tenderers are to confirm compliance to Specification by indicating **Yes/Partial/No** on **Schedule 15G** of the tender. If No, tenderers must provide comments / mitigation in relevant column. The Bid Evaluation Committee will assess whether the mitigation/ solution provided conforms to the scope required.

Document Management - Functional Requirement Category-	Document Management - Functional requirement
Document management *The Electronic Document Management System (EDMS) must be able to provide, or integrate with, document management facilities to ensure records management functions are seamlessly supported.*	**Control** • The system with document management facilities must make a clear and obvious distinction between digital documents and registered digital records. • The system must provide options for registering all unregistered digital documents in a particular folder or folders as formal records, in a single process. • The system must allow automatic deletion of all unregistered digital documents in a particular folder in one process, or after a set period.

	Capture
	The system with document management facilities must be able to:
	• capture and register in one process:
	   ○ a newly created digital document; and
	   ○ a digital document already existing in the document management environment.
	• capture a digital document and allow the option of completing the registration process at a later time.
	• allow users to transfer smoothly between the document management environment and the system to register a digital document as a record.
	• Automatically create versions of digital documents, without automatically creating a new digital record.
	• copy a digital record to make a new digital document, ensuring the digital record remains unaffected.
	• manage versions in a tightly bound relationship, to support drafting and ensure the integrity of the digital document as a whole.
	• provide options for registering some or all versions of a digital document as digital records.

	Access and security • The system with document management facilities must not allow ownership rights from the document management environment to apply to a registered digital record. • The system with document management facilities must not allow a registered digital record to be checked out, where this would allow the alteration of record content in any way.

Document Management - Functional Requirement Category-	Document Management - Functional requirement
	Disposal • The system with document management facilities must be able to detect digital documents in any folder due for export or transfer and notify the RM System Administrator. • The system with document management facilities must enable digital documents to be registered as records before export or transfer. • The system with document management facilities must be able to export only registered digital records. • The system with document management facilities must automatically destroy digital documents when the digital records to which those documents relate are destroyed after a successful transfer process.

	Searching and retrieval
	• The system with document management facilities should have the ability to retrieve documents along with records, using the same search interface.
	• The system should allow an authorised user to configure the retrieval of documents to:
	  ○ the latest version only;
	  ○ selected versions only;
	  ○ only those versions registered as records; or
	  ○ all versions of the document.

	Metadata • The system with document management facilities must support the mapping of digital document metadata to digital record metadata, as set out in the Record and Document Metadata Standards. • The system with document management facilities must support the definition of templates for common digital documents, and the allocation of different metadata set for each template. • The system with document management facilities must ensure that any metadata captured in the document management environment is managed under the requirements of the system specifications, to ensure its authenticity. • The system with document management facilities must allow metadata to be captured from a user at the time of capture and registration.
Conversion to a Record	**Converting a Document to a Record** • The system should allow the user to right-click on the document once selected and then select the option to convert the document to a record or the system should provide a similar icon-driven event to trigger the conversion. • All related metadata and taxonomy information must be carried forward with the document in the creation of the record

Compliance
The system must meet relevant local, national, and international requirements for document management
	Legislation
	• Consideration for the Protection of Personal Information Act promulgated in 2019 and effective in 2020, and the Promotion of Access to Information Act with input from City Legal as a stakeholder
	• The system must support compliance with the document management, evidential, privacy and access provisions of all relevant South African legislation and regulations, including and not limited the to the following:
	  ○ Policy Framework for the Government-wide Monitoring and Evaluation Policy System 2007;
	  ○ Minimum Information Security Standards of 1996 (MISS);
	  ○ Minimum Interoperability Standards (MIOS) for Information Systems in Government;
	  ○ Promotion of Administrative Justice Act (PAJA) 2000 (Act 3 of 2000);

Document Management - Functional Requirement Category-	Document Management - Functional requirement
	- o Promotion of Access to Information Act (PAIA) 2000 (Act 2 of 2000); - o Protection of Personal Information Act (POPI) 2013 (Act 4 of 2013); - o Electronic Communications and Transactions Act (ECT) 2002 (Act 25 of 2002); - o Public Finance Management Act 1999 (Act 1 of 1999); - o Municipal Finance Management Act No. 56 of 2003 (MFMA); - o Law of Evidence Amendment Act 1988 (Act 45 of 1988); - o Companies Act; - o Financial Intelligence Centre Act; - o Financial Advisory and Intermediary Services Act; - o The Income Tax Act; - o VAT Act; - o Customs and Excise; - o Stamp Duties Act; - o Prescription Act; - o Insolvency Act; - o King IV Code. - o
	Standards - Updates to ISO/DIS/SANS 16175: Information and documentation - Processes and functional requirements for software for managing records and to Relationship between the ISO/SANS 16175 series of standards and other products of ISO/TC46/SCII: Archives/Records Management - The system should support compliance with all applicable South African and international standards. The standards do not replace the requirements contained in the National Archives and Records Service of South Africa Act (Act No. 43 of 1996, as amended) (NARSSA Act) but affirm and support the statutory requirements. - Some, and not all, of the applicable standards applicable to document management are listed below: - o ISO (SANS) 15801:2017 – Document management - Information stored electronically - Recommendations for trustworthiness and reliability; - o ISO (SANS) 18492:2005 Long-term Preservation of Electronic Document-Based Information; - o ISO (SANS) 17799:2005 – Information Technology Security techniques – code of practice for information security management; - o ISO (SANS) 14721:2012 – The Open Archival Information System (OAIS) Reference Model: Introductory Guide; - o ISO (SANS)19005-1:2005 - Document management - Electronic document file format for long-term preservation Part 1: Use of PDF 1.4 (PDF/A-1); - o SANS 19005-2:2011 - Document management - Electronic document file format for long-term preservation Part 2: Use of ISO 32000-1 (PDF/A-2); - o ISO (SANS) 25964:2011 - Thesauri and interoperability with other vocabularies – Part 1 Thesauri for information retrieval; - o ISO (SANS) 25964:2013 - Thesauri and interoperability with other vocabularies – Part 2 Interoperability with other vocabularies.
	Guidelines - Consideration should also be given to the CCT's policies as well as the policies and protocols as specified by the Western Cape Government's WCARS (Western Cape Archives and Records Service). - The list below contains some of the guidelines that the system needs to adhere too and enforce: - o The DOD 5015.2-Standard; - o CCT Records Management System and Procedure;

Document Management - Functional Requirement Category-	Document Management - Functional requirement
	o CCT Information Security SOP; o CCT Electronic Communication SOP; o CCT Electronic Mail Usage Rules; o CCT IT Continuity SOP o CCT Business Continuity SOP; o CCT Data Strategy; o WCARS Digital Preservation Policy; o WCARS Naming Convention Protocol; o WCARS Digitalization Policy.

13.4.2.3 SUMMARY OF THE SYSTEMS MANAGEMENT AND DESIGN FUNCTIONS

Below is a list of the minimal core System Management and Design primary functions that the new integrated RM&DM&CM solution should provide:

- Usability
- Reporting
- System administration
- System design

These functional requirements definition is related to **SCHEDULE A** in section **(5) Price Schedule** of this tender document. Refer 2.2.1.1.6 of the Eligibility Criteria. Tenderers are to confirm compliance to Specification by indicating **Yes/Partial/No** on **Schedule 15G** of the tender. If No, tenderers must provide comments / mitigation in relevant column. The Bid Evaluation Committee will assess whether the mitigation/ solution provided conforms to the scope required.

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement
Usability *The RM&DM&CM system must be logical to operate and simple to learn, taking into account the differing needs and abilities of potential users.*	**User interfaces** • The system must provide a user interface that complies with the accepted standard rules for the operating system or platform on which it will operate and where it supports a web browser interface, it must meet internationally accepted guidelines for web design. • The system user interface must be presented consistently across all windows, menus, commands and other facilities and need to provide a single sign-in and access to the objects, documents, records and case management modules.

	Usability of system functions
	• The system must produce meaningful error messages that offer a simple method of correcting the error or cancelling the process supported by an online context-sensitive help facility, including help on the use of the records classification scheme where supported as well as a spell-check facility at all data-entry stages, including searching.
	• The system must ensure that minimal movement between screens is required to perform system operations and must make consistent use of function keys, hot-keys and short-cut keys across all components of the system.
	• The system must be able to hide system functions from users who do not have permission to use them and also prevent users from carrying out the initial steps of a process they will be unable to complete due to functional permission restrictions.
	• The system must ensure that its facilities are as intuitive and easy to use as possible by allowing:
	   o functions to be performed with as few mouse clicks or keystrokes as possible; and
	   o the completion of routine functions from one screen.
	• To allow records to be captured by the system with minimal user intervention, the system must be capable of integrating or interfacing with (as required):
	   o standard office suite applications;
	   o standard electronic messaging systems, such as email, SMS and WhatsApp (or any other social messaging system) clients;
	   o other mainstream applications already installed, and particular business information systems used by the organisation.
	• The system must be able to generate an electronic message from within the system, to attach:
	   o digital records and documents;
	   o metadata; and/or
	   o active pointers to records and/or metadata.

Reporting *The system must be able to produce reports on system activities and the status of objects within its control, for management, statistical and general purposes.*	**Report management** • The system must provide a reporting capability to produce management, statistical and ad hoc reports on system activity based on restriction on end-user's access to selected reports, or the reporting function in general. • The system must allow reports generated to be saved, modified and re-used in the future and it must also allow reports generated to be easily exported from the system using one or more common data formats (such as plain text, comma-separated value, or tab-delimited computer file types). • The system should be able to export the information in JSON and XML standards or any industry-accepted standard in the future.

	Reporting on classification tools
	• Where the system supports a records classification scheme or business classification scheme, it must be able to generate a report comprising:
	    o the entire scheme; and
	    o a part of the scheme (e.g., a specified function and its related activity in terms, indicating the relationship between terms in a hierarchical format.

	Reporting on folders and records
	• The system must be able to produce reports listing:
	    o all folders classified within the records classifications scheme; and
	    o all folders classified in a section of the records classification scheme, structured according to the hierarchy of the record plan or other classification tool.
	• The system must be able to produce statistics for the number and location of:
	    o digital records by application type and version; and
	    o digital records and folders by specific access and security controls.
	• The system must be able to produce a report listing the details and outcome of any migration process, to ensure the integrity of digital records.
	• The system must be able to report on the size and remaining capacity of its digital record stores and repositories.

	Reporting on user activity
	• The system must be able to report the actions carried out by a particular user, or group of users, during a specified date range.
	• The system must be able to generate a list of all, or a subset of, user profiles known to the system.
	• The system must be able to produce statistics for the number of records
	    o and folders created by a user or group of users for a defined period; and
	    o viewed by a user or group of users within a defined period.

	Reporting on access and security
	• The system must be able to report all attempts at unauthorised access to the RM System Administrator.
	• The system must be able to
	    o generate a report based on selected access controls and security controls.
	    o report on all alterations to access permissions, access controls and security controls, within a specified period.
	    o to generate a list of all, or a subset of, user access groups known to the system.

	Reporting on disposal activity
	• The system must be able to produce reports on all disposal activity undertaken by the system.
	• The system must be able to produce a report listing:
	    o all disposal classes currently defined in the system;
	    o all digital records, folders or other record plan entities (where supported) to which a particular disposal class is currently applied;
	    o all objects for which a particular disposal action will occur, over a given period; and
	    o all objects due for disposal within a given period
	• The system must be able to report on all objects subject to a disposal freeze.
	• The system must be able to produce:
	    o statistics of review decisions over a given period;
	    o a report detailing any failure during export of objects from the system, identifying objects that have generated processing errors or were not successfully exported;
	    o a report detailing the outcome of a destruction process, detailing all objects successfully destroyed and identifying those objects which that were not successfully destroyed; and
	    o report on the volume and types of objects that are overdue for disposal.

System administration
The system must provide facilities for the ongoing maintenance and support of the system, and the data it manages. Some of these functions may be provided by the operating system, database management system or other applications linked to the system. Clearly indicate if the system provides the functionality or if it relies on other third-party capabilities to provide these functionalities
	Data processes
	• The system must automatically invoke checks that system operations are successfully performed on transactional data.
	• The system must support automatic data validation rules.
	
	Deletion of records (For information on records destruction, see the Disposal section)
	• The system must allow a default or option that prevents any user or RM System Administrator from changing, moving or deleting in an ad hoc manner a digital record or object once captured.
	• The system must ensure that any function to delete digital records or folders on an ad hoc basis (outside the disposal process) is restricted to the very highest level of RM System Administrator.
	• Where the system allows deletion of a digital record, folder or other record plan entity, it must:
	    o ensure that no objects are deleted if their deletion would result in a change to another object;
	    o notify the RM System Administrator of any objects linked to the object about to be deleted;
	    o seek confirmation from an authorised user before proceeding with deletion;
	    o delete the entire contents of the object;
	    o record the deletion comprehensively in the audit trail; and
	    o produce an exception report.
	• The system must support the retention of metadata for digital records, folders and other record plan entities that have been deleted.
	• The system must allow a RM System Administrator to amend user-entered metadata, as part of an audited procedure.
	• The system must prevent the deletion of metadata that is associated with an object under the control of the system.

	Storage
	• Subject to the metadata requirements, the system must support the storage of digital records and associated metadata either:
	    o together in a digital repository that is an integrated part of the system; or
	    o separately, with records maintained in the native software environment, and metadata under the control of a system.

	• The system must provide facilities for monitoring digital repositories and must warn a RM System Administrator when storage limits are about to be reached.
	• The system must be able to prevent or resolve any conflicts caused by changes to storage locations.
	• The system must support automated back-up and recovery facilities for all (or selected) entities, metadata, audit trails and configuration settings held by the system based on the manual configuration of the frequency of back-ups, and elements of the system to be backed up.
	• The system must allow a RM System Administrator to restore the entire system
	○ from backups, maintaining full data integrity to ensure business continuity;
	○ from the most recent back-up to the point of system failure.
	• The system must provide notification of any data updates that were unable to be recovered or rebuilt.
	• The system must support the identification of vital records that are critical to business continuity.
	• The system shall provide the capability to automatically synchronize multiple databases and repositories.
	Preservation
	• The system must be able to manage digital objects according to the minimum mandatory requirement of this document over time, to ensure their integrity and support long-term preservation.
	• The system must support automatic and manual mapping to and from the system metadata fields.
	• The system developer must have a routine in place to ensure that digital records remain accessible and retain their integrity after a system upgrade.
	• The system must use and house all storage media in environments that are compatible with expected life, and within a tolerance of the media manufacturer's specification.
	• The system must ensure that all tailored modifications are brought forward and are operational when system upgrades are implemented without the need to recreate and redevelop these customisations again.
	• The system must be able to migrate digital records, folders, physical registry files and other record plan entities (where supported) following the requirements for export and bulk import listed in the section above.
	• The system must be able to perform bulk conversion of digital records to other media and/or systems in line with the standards relevant to their format(s), for example, PDF/A for long term preservation and PDF/J for architectural documents.
	• The system must ensure that no data is lost or corrupted during system upgrades, migration or conversion.
	• The system must support periodic refreshing of storage media, to guard against media degradation.
System design *The system design must support response times and levels of system availability that meet current and projected user requirements.*	**Performance** • The system must provide a stable and flexible architecture that can grow to meet changing business needs, and continue to meet the recordkeeping requirements appropriate to its particular implementation. • The system must be able to consistently perform all functions to a specified standard which meets business needs and user expectations. (see the non-functional requirements for some parameters). • The system must demonstrate acceptable response times for commonly performed functions, under normal operating conditions. Benchmark measures for performance may include the time taken to:
	○ display a graphical view of the record plan;
	○ store standard documents at capture and/or registration;
	○ return a search response for a simple query;
	○ return a search response for a complex query; and

		o display text missing. The system must provide: • Centralized back-up and restore • GUI administration accessible to Administrator • Out-of-the-box Load management • Supports Network Load Balancing and Clustering • High throughput and scalability

Scalability
- The system must be capable of controlled growth, to continue to meet anticipated organisational needs over time.
- The system must demonstrate its capacity to handle the projected needs of the organisation, whilst maintaining the expected performance measurements stated previously. Indicators of scalability may include whether:
    - o the maximum size of the digital repository will be able to accommodate the expected total number of records;
    - o the number of geographical locations across which text to complete which the system will meet anticipated organisational needs;
    - o the total number of users that can be supported will accommodate predicted staff increases;
    - o the amount of systems administration and re-configuration down-time required to support projected numbers of records and users during the first five years of operation falls within acceptable parameters; and
    - o the amount of downtime required to make bulk changes to organisational structures, classification tools and user roles (with the number of folders, records and users anticipated after five years of operation) will fall within specified acceptable parameters.

Reliability and control
- The system must demonstrate its capacity to remain available and operational, as required to meet business needs. Measures for reliability may include:
    - o specified hours of the day, or days of the year, during which the system must be available;
    - o range of planned or unplanned downtime that can be tolerated; and
    - o the acceptable period required to restore the system from back-up in the event of system failure.
- The system must have the ability to enforce data integrity, referential integrity and relational integrity at all times.
- The system must ensure that all entities (e.g., folders, records, extracts) are allocated a unique system identifier.

13.4.2.4..CASE MANAGEMENT

Case management generally implies following a well-structured process. This in turn often means that it will be beneficial to apply workflow technology. Workflow can be defined as "The automation of a business process, in whole or in part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules."

In this definition, a "participant" can be a user, a workgroup (a team), or an application system. The Workflow requirements as described here relate only to the definition of a standardised business process external to the RM&DM&CM. Consequently, processes defined for delivering RM&DM&CM functionality will not generally satisfy these requirements.

Many of the additional requirements for case management are related to the need for an RM&DM&CM to integrate closely with such systems.

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement
CASE MANAGEMENT *Refers to an application designed to support a complex process that requires a combination of human tasks and electronic workflow-enabled through workflow, management collaboration, storage of images and content, decisions, and processing of electronic files or cases*	**Workflow Engine** The system must have a workflow engine to support different types of document routing mechanism including: - Sequential routing -Tasks are to be performed one after the other in a sequence. - Parallel routing - Tasks are split among multiple users and then merged as a single composite work item through the support of conditional merging of the multiple parallel activities. - Rule-based routing - One or another task is to be performed, depending on predefined rules. - Ad-hoc routing - Changing the routing sequence by authorized staff with the appropriate access and rights. The system should support the registering and configuring of third-party applications.
	Process Design - The system must have a built-in Graphics based workflow designer to design Business Processes based on BPMN ver2.1 standard. Any process design or modification should be performed without the need for programming expertise, - The Process designer must have an intuitive interface to assist in the design of complex rules and conditions for workflow routing. - The system shall allow the creation and the storage of sub-processes and allow the re-use of the sub-processes across the Enterprise to enable uniformity in process actions and the enablement of agility. - The system should provide a facility to define multiple archive stages to archive selected documents and indexes in the underlying Document management system at any stage of the workflow process. - The system must provide the capability to define hold stages so that a particular instance of the workflow can be kept on hold for specified interval based on the pre-defined condition as well as the facility to define the conditions for resuming the instance that is in the hold stage. - The workflow management system shall support the definition of roles and allow many-to-many relationships between users and roles to be defined. - The system must provide the facility to assign ad hoc tasks at runtime to users.
	Form Designer - The system must provide a built-in facility to design custom forms that can be attached at one or more stages in the workflow. - The Form designer interface shall enable the user to define text boxes, Combo boxes, radio buttons, Dropdown etc. - The system shall support field-level calculations at form level as well as scripts to control field level validations. - The system shall provide a facility to define variables in the process or in external database tables, which can be linked to fields defined in the form for efficient data entry.

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement
	Exceptions Handling • The system must enable the CCT to define exceptions per stage if required, which shall dynamically alter the process flow on execution. • The RM Administrator shall have the ability to grant rights to raise and clear exceptions at different stages of the process annotated with user comments. • The system must be able to raise triggers based on exceptions. • The system should provide a facility to raise automatic exceptions based on pre-defined conditions. • The system shall track all the exceptions raised in the course of the process and shall maintain the history of that with the user's name, date, time and comments. • The system must be able to differentiate process instances with and without exception • The system must have a built-in Rule Engine that will be used for defining business and process rules.
	Triggers Handling • The system must allow the authorised users to define custom triggers like Emails, Word template or launching executables on predefined conditions. • The system must have a facility to define custom trigger templates that can utilise static and dynamic data. • The system must have the ability to generate event-based triggers that will automatically send emails/ fax, generate responses, invoking data forms to capture data as well as invoking communications with external systems. • The workflow management system must send an email notification to a user when the user is not logged into the workflow management system. If the user clicks on the URL in the email, then the system must automatically launch the Workflow management system and present the user with the task to perform.

	Process Monitoring and Reporting
	• The workflow management system must track and be able to display in graphical and in tabular format the worktime status, the date/time the task started and ended as well as the creation and archival date of the documents.
	• The system must provide the users with the ability to configure without requiring any coding the dashboard for specific roles e.g., dashboard for a director, a dashboard for Administrator, etc.
	• There should not be any limit on the number of reports that can be created in the system.
	• The User must be able to drill down into a report for specific information analysis.
	• The workflow management system shall support the generation of statistical and management reports like:
	    o Average Process Time Report
	    o Diversion Report
	    o Exception Details Report
	    o Expired Work-item Report
	    o Number of pending files
	    o Participant Processing Time Report
	    o Participant Report
	    o Process Definition Summary Report
	    o Process History Report
	    o Time is taken to complete each task
	    o User Performance Report
	    o Performance comparison reports.
	    o Total turnaround time and
	    o Delay report for complete process or specific work stages
	• The system must incorporate an administration module to configure the user, groups, queue related to a process. It is recommended that these setting must be captured in the central RM&DM&CM configuration tables.

Systems Management and Design Functions - Functional Requirement Category-	Systems Management and Design Functions - Functional requirement
	User Management and Security • The workflow management system shall support integration with Lightweight Directory Access Protocol (LDAP) for domain-level authentication and single sign-on or whichever future Access management protocol that the CCT will use. • The workflow management system shall support integration with database authentication as per the CCT's protocols. • The workflow management system shall be capable of giving access rights to users/groups on work stages, documents, forms and data fields. • The workflow management system shall support extensive password validations i.e. locking of a user account after the specified number of unsuccessful login attempts, password history, password expiry, passwords must be alphanumeric and of minimum character length etc. • The workflow management system shall support SSL, HTTPS and any other session timeouts that might be required by the CCT.
	Administration and System Management • System and Business administration access rights need to be different to ensure users are managed by the business and the system variables by the RM System Administrator.

	Business rules management
	• The system should support a business analyst to define business rules, associate the rules with business processes and business rules management.
	• The platform must come with tools that allow business rules to be easily authored by business users without any technical help from IT.
	• The system must have the ability to expose rules as APIs/Web service to be consumed by 3rd party applications.
	• The system must also provide the following functions:
	  ○ Rule versioning management
	  ○ Web-Based User Interface for Business Users to Edit Rules
	  ○ Manage an unlimited number of rules.
	• The system must have a master data management (MDM) module where all process-related master tables can be defined via a user-friendly GUI interface.

	Audit Trails
	The system should support capturing of an audit trail for the following but not limited:
	  ○ Workflow events
	  ○ User assignments/releases
	  ○ Notifications

13.4.2.5 DIGITAL SIGNATURE SYSTEM

The CCT as part of its initiative to move towards a digital business model with the paperless or paper-less environment would require a Digital Signature system that provides the necessary functions as per the Electronic Communications and Transactions Act, 2002 of South Africa. Depending on the type of transaction and the financial and legal liability, either the

- Electronic Signature
- Digital Signature
- Advanced Digital Signature

This system will update and interact with the DMS, RMS as well as the Case Management System (CMS). It must also be able to be configured to operate with the current legacy systems as well as the future systems.

The application will also cater for interaction with the residents and citizens as well as for internal usage within or between departments to increase efficiency and compliance.

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature
Onboarding and Registering *Onboarding is the process of registering new and existing customers, ensuring that they access all the services and products contracted in a simple and fast way, integrating into the company's customer base. This forms part of the 3-way authentication required in some digital signatures.*	The system should allow for proactive onboarding of signatories as per the customer's/signatory's subscriber agreements. • Ability to onboard a signatory before documents needing to be signed. i.e., proactively onboarding customers/signatories, as soon as the subscriber agreement is signed, to ensure a seamless process when signing.
	The system is to allow customers/signatories to register on the signing platform with appropriate login credentials which they can use going forward. This includes the customer agreeing to the terms of the Advanced Electronic Subscriber Agreement (AESA). • New customers/signatories should be able to register a profile with the necessary details (ID number, name, surname, email address, cell phone number, etc.). • Security questions are also to be included as part of the registration process. • Advanced Electronic Subscriber Agreement (AESA) - Once signed, the digital copy is to be automatically uploaded to Record Management System under the correct taxonomy.
Signatures – including multiple signatures	The system should allow for multiple signatories to sign a document/s. • Email notifications informing signatories that their documents are ready to be signed should be sent in the order that the signatories were captured. • Only once the first signatory has signed all documentation in the pack, should the next signatory get a notification that they can commence with the signing process and so forth (for the remaining signatories).
	• The system should only upload the document sets that pertain to the electronic method of signing. • The system should have the ability when drafting the contract to identify whether the client is signing electronically or face-to-face to ensure that the document set has witness requirements or not according to the customer's/entity's signing method/preference indication. • The different versions of the contract document should be saved in the Document Management System with version control and the required metadata • Once the final signature is received, then the contract record must be saved to the Records Management system and logged to make the document immutable.

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature
	Once a document has been signed, the system should have the ability to apply the customer's/signatory's initial on each page in the document that was signed, • Once the customer/signatory has signed the document, the system must automatically apply their initials on each page within that document
	The system should allow signatories to view all past signed contracts. • Signatories must always be able to log back into the system and view all previously signed contracts or use the RMS to view these records
Customer communication	The system must send an email and/or SMS to the customer informing them that their documentation has been drafted and is ready to sign. • Communication must notify the customer/signatories to access the platform. • In the case of multiple signatories, the same communication is to be sent to all relevant parties.
Use of One-Time-Pin (OTP)	The system must make use of a one-time pin (OTP) sent to the customer/signatory for accessing the platform. • The customer/signatory should be able to choose if they would like the one-time pin (OTP) sent to their cell phone number or email address. • If the customer/signatory is a new user, the OTP should be sent to the cell phone number or email address that the customer captures as part of the registration process. • If the customer/signatory is an existing registered user, the OTP should be sent to the cell phone number or email address on record for that customer.
	The system should allow for signatories to sign documents separately (one at a time) and all at once (bulk signing), using an OTP (one-time-pin) as validation. • A signatory should be able to select each document and be able to sign them separately. • A signatory should also be able to select and sign multiple documents at once. • An OTP must be entered by the signatory as validation before the signatures are applied to the document/s.

Different Electronic signature requirements	The system must make use of Advanced Electronic Signatures (AES) for customers that are required to sign collateral or any documentation related to transferring assets. Where the customer is not required to sign collateral, the use of a standard digital signature is acceptable. The CCT needs to define the digital signature policy to indicate what type of signature is required for what type of transaction.
	• An advanced electronic signature consists of a digital certificate confirming the identity of the applicant, with an added face-to-face verification mechanism, as well as 3-factor authentication, which includes[1] :
	    I) Biometrics, such as fingerprint and iris scan;
	    ii) Pin, password, passphrase or secret question; and
	    iii) Key, device
	• A citizen can make use of digital signatures for signing purposes, where no collateral is required.
	• If at least one document requires signing with an AES, the customer should make use of AES for all other documents within that contract pack to provide a consistent user experience.

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature
Digital Stamp	The system should create a digital stamp to reflect the signatory's signature. • The stamp should display the date, time, time zone, customer's full name, email address and mobile number as per the ECT act of 2002 • Where possible, the system needs to record the unique identifier/s for the device on which the customer/signatory is signing the document.
	The system should be able to capture the customer's/signatory's location at the time of signing. • The customer's location can be captured based on the IP address for the device that the customer is using, alternatively, the customer can enable location services on their signing device. • The signatory's location is not to be displayed on the stamp but is still to be recorded in the metadata. • In the cases of cell phone signatures, it is recommended that the GPS coordinates of the cell phone be recorded as part of the metadata.
Tracking control	The system must allow for the signing progress to be tracked • Internal users of the system should be able to track any outstanding signatures, fields, etc. • Internal user can track who has or has not signed the documents and the outcome i.e., accept or reject. The version control and metadata in the Document Management system can be utilised to provide the tracking control.
Integration with DMS RMS and Workflow Engine	The system is to allow for documents to be appropriately stored. • Documents are to be pushed to the DMS (and filed under the correct taxonomy) and be stored on the DMS. • Document metadata is to also be recorded as part of this storage process. • Once all the signatures are received, the document needs to be converted to a record and saved in the RMS. The Case Management tool can be used in instances where cases were created to perform the document to record the transformation process. The system should allow for seamless integration with the workflow engine
Expiry Date	The system should allow an expiration date for signing all required documents. • An internal user should be able to set a validity period during which the customer needs to sign the documentation, after which the documentation will expire. • Alternatively, the business rules in the Case Management system can be used to auto allocate the expiry dates. • The expiry period for OTP's will also have to be enforced and applied by the system if it forms part of the three-way validation process.
	The system should send an appropriate reminder to a signatory if they do not complete the signing process once they commence their signing session • A reminder is to be sent out to the customer within a specified period, e.g. one hour after commencing their signing session, should they not complete the full signing process.
	The system should allow for an internal user or an internal system to proceed with the cancellation of the document signing process. • In the case where documents need to be updated or redrawn, an internal user should be able to cancel the signing process until all prerequisites have been met.

Systems Management and Design Functions - Functional Requirement Category-	Functional requirement – Digital Signature
Customer rejection procedure	The system should allow for the customers/signatories to reject a document that requires signing. • The customer reserves the right to reject a document if they are unsatisfied with its contents and agreements therein. • In the case of multiple signatories, the rejection of a document by one of the signatories should cancel the signing process for all signatories. In such a case, all relevant parties to be notified of the cancellation/rejection, as well as the reason for rejection. The documents signed by signatories before the rejection should be void. This business rule is applicable for CAF and Co-debtors and Sureties. • A rejection update should be reflected on the DMS, where any relevant CCT stakeholders can access the information based on a reference number.
	The system should allow the customer/signatories to provide a reason for the rejection of a document. • Reasons should be provided as a selection list of predefined reasons from which the customer can choose. *These reasons will have to be defined by the CCT and signed off.* • A 'My reason is not listed' selection should be made available to the customer. If the customer/signatory selects this option, a free text box is to appear that allows them to capture additional detail. This text box is to have a character limit.
Notes	The system should allow customers to add notes for changes they would like made. These notes can be entered in the case management system or the digital signature system but the notes should be reflected in the case management system. • Customer to be able to make notes on the document for amendment requests. • Customers should be allowed to make smaller, immaterial changes on their own which can be noted in an addendum to the contract. In this case, the customer should be able to continue with the signing process. The types of changes that the customer can be allowed to make are to be defined by respective Compliance and Legal stakeholders, as well as appropriate business rules. • Any changes that are made by the customer must also be pulled through and updated on the master record on the ERP system.
Consolidated signature page	The system should have one consolidated signature page that needs to be signed, which represents all documents in the contract pack. • Signature page to reflect all documents that have been signed as well as all signatories that have signed (in the case of multiple signatories). • Should include a summary of the contract (amounts, etc.).
	The system should have a consolidated signature page for every document that needs to be signed. • Once the documents have been signed, each document should have a page at the end where each signatory's signature will be reflected.
Additional requirements	The system should also comply with the following requirements: • It should enable the user to sign the file types they typically use (e.g.PDF, DOC, DOCX, TXT, XML, etc.) • The system must integrate with the existing applications or those that might be used in the future, e.g., contract management, HR services. • The system should allow the CCT to brand the front end to reflect the corporate identity

13.4.2.6 WORKFLOW ENGINE

The Workflow engine would be required if the application workflow functionality provided in the Document Management, or Record Management or Case Management is not capable of providing an enterprise workflow solution.

The functional requirements listed below must be read in conjunction with the functional requirements for the workflow requirements in the Document Management, or Record Management or Case Management modules to have a complete view of the functional requirement for the RM&DM&CM functionality requirements for the CCT.

Core Functional Requirement Category	Core Functional Requirement

Workflow Engine functionality
Workflow core elements are *events, triggers* and *routing*.
	The Enterprise Workflow engine should be able to:
	• Manage and support event types:
	    o Create, Retrieve, Update or Delete a token
	    o Status Changes (may or may not include routing)
	    o Approval Activity (to include approved, declined, need more information etc.)
	    o Notifications
	    o eSignatures (associated with statements of certification, recognition of review or receipt, document management etc.)
	    o Legal statement of acceptance or contract - Policy issues related to e-signature and legally binding actions that may require a higher degree of authentication than normal processing.
	    o Batch Processes
	• Handle triggers:
	    o For each event type listed above
	    o Scheduled (specified date/time)
	    o Time-based intervals (window of time from an event or a scheduled trigger)
	    o Condition-based (i.e., a threshold reached)
	    o Manually launched
	    o Launch another workflow and or be launched by another workflow
	• Routing options:
	    o Parallel paths (two types)
	        ▪ Simultaneous routing path (may include approvals) where the triggers and events are not dependent upon each other until they reach a common event.
	        ▪ Simultaneous routing path (may include approvals) where the triggers or events are dependent upon each other.
	    o Conditional
	        ▪ Routing path to be defined by event or token attributes.
	    o Ad-Hoc
	        ▪ Ability to escalate or re-route, add to, modify the routing process (with specific security permissions)
	        ▪ Ability to spawn localized or sub-process workflow routing within an event or trigger.
	        ▪ Support "black-box" routing where user manages trigger or event rather than allow workflow engine to route.
	            • Manual routing of token
	            • User-defined'

Business Rules *Any enterprise workflow implementation must support all existing business rules within existing workflow systems or processes for those systems that will replace or re-factor*	The workflow should support business rules with: • High level of complexity (more than 15 layers of dependent rules) • Ability to specify business rules for the token type, Role, User, metadata element, period (or any combination of above rules) etc. • Control overviews of workflow elements (based on modifiers specified above) (Example: a specific business rule may define that watcher within ORG code X can only view the approval details of a token at their access level or below.) • Allow for ad-hoc modifications to business rules with defined security access. o Currently, existing UWL workflows allow ad-hoc changes per token but do not allow those ad-hoc changes to be permanently applied as a new rule.

Core Functional Requirement Category	Core Functional Requirement

their workflow to use the enterprise tool selected	• Ability to add business rules for a new token type or ORG/Role/User etc. without code changes (for example: with the use of an administrative user interface).
	• Ability to define escalation route(s), triggers or events for a specific token type or attribute.
	• Ability to provide business rule templates and copy/clone options of existing business rules.
	• Support the elimination of "empty" approval nodes on the workflow process.
	   ○ On set-up warning of a rule resulting in an empty approval event.
	   ○ When a contact removal results in an empty node a notification for reconciliation is generated.
	• Require tools and/or ability to build custom workflow solutions

Notifications *Notifications provides a means of delivering a message to a set of recipients. The messages can be sent via various communication channels such as email, text message, tasks on a user's calendar, phone call, etc.*	Workflow notifications should be able to: • Automatically notify individuals of tasks that they must perform. (Example: Approve token, review supporting information, respond to a request, etc.) via various mechanisms available through the workflow engine. • Automatically notify the creator of the token when task completion or outcome occurs (if specified by the user, role or business rule). • Support time-based triggered notifications. • Record when system messages are sent and retain copies of sent messages. • Fetch data (any/all data sources) and include it in a notification message. • Create or include a hyperlink to a token defined destination within application or workflow engine. • Support delivery verification with a delivery receipt where needed/requested. • Security options for control of what type of messages can be sent via certain mechanisms (using reliable messaging that provides the underlying infrastructure for security). • Users should be able to configure notifications preferences to support their desired delivery method, display, etc.
Audit & Historical tracking *Audit and history tracking enable organizations to construct a meaningful picture of what has or has not happened to a token. It also provides a greater level of accountability, allowing organizations to determine who made what changes when.*	The audit and tracking within the Enterprise Workflow tool should be able to: • When a token is passed through the workflow each status and activity change should allow for user comments. • Record the ID of the person or system who performs any activity in the system, as well as when and where the activity takes place (within what application or what portal, etc.). • Display a record of all the statuses a token goes through, and date/time the status of the token change. • Maintain and display a snapshot or version of the token at key routing points within the workflow. – This may be handled with other mechanisms such as "track changes" or capture only with certain data field/type changes. • Include notification information within the audit and history trail ○ Who, when (trigger), how and a copy of message text to be included in the history.

Presentation Layer
An enterprise workflow solution must be transparent to its users. Users need to know the status of tokens as they move through the workflow.
	The presentation layer needs of an enterprise solution must allow the following features:
	• Different portals for the different defined roles
	   ○ Options to extract data to provide to a system outside of workflow to deliver the information to the public or read-only views.
	• End-user applications may require their own separate presentation layer within their application.
	   ○ If the workflow tool is used across distinct applications, the user should have seamless navigation to the workflow features and functions.
	   ○ The workflow tool should allow for the branding of an individual application instance (i.e., logo, colours, etc.)
	• Information about the state of each token in the workflow is easily accessible.
	• List of tokens and their metadata that allow for sorting and filtering.
	• Profile of users or roles to allow for view definitions.
	• Graphical representation of workflow process and progress.

Core Functional Requirement Category	Core Functional Requirement
	• Provide colour-coding options for activities, status and flow as required for escalation and critical paths, etc. (Colour coding should enhance data, but not be the only way of defining status; there must be support for screen readers or colour-blind disabilities.) • Allow for control of notification preferences through the presentation layer (rather than through the workflow configuration). (Examples: Daily Digest, RSS, etc.) • Expose audit and history trail of the token (view to be defined at the user or role or application level). • Presentation layer accessibility should be defined by workflow security settings and desired exposure (Web, desktop, embedded in another system, etc.).

Security
 	
Workflow security must support CCT's authentication and authorization standards. Authentication is a process of determining whether someone or something is, in fact, who or what it is declared to be Authorization determines a user's access to information, services, etc. with defined policies within an application.
	• Security for workflow should:
	• Integrate with single sign-on solutions as described in the document.
	• Integrate with RM&DM&CM roles.
	• Workflow roles must be mapped to security roles.
	• Support existing workflow roles within implemented workflow products and allow expansion to the current access (each workflow process may have its own set of roles and needs – see individual process requirements).
	    o Creator
	    o Stakeholder
	    o Approver
	    o Approver Delegate
	    o Leader
	    o Reviewer
	    o Watcher
	    o Viewer
	    o Public (for external exposure if desired) – Read Only
	• Should have a standard set of security roles, but also allow configurable workflow roles.
	    o Workflow roles (as listed above) are to interact within the workflow engine. These should be configurable based on the needs of the specific process.
	• Display different views for different security roles.
	• Provide the ability to set an encryption or security level for a token type, token data element, extract files or attachment to meet confidentiality requirements for each unit.

Integration Points.
 	
See the integrations standards for the CCT that the system needs to adhere to for specific guidelines
	Systems (Databases, etc.)
	Enterprise Workflow engine may require integration with the following systems:
	• Enterprise Data Warehouse
	• Other Workflow Systems
	    o SharePoint (HR, etc.)
	    o ERP solution
	    o Document Management system
	    o Record Management system
	    o Case Management System
	    o Digital Signature system
	    o Etc.
	• Standards-based systems (APIs) (Business Applications examples below, not exhaustive)
	    o Procurement
	    o HR
	    o Finance
	    o Payroll
	    o Etc.
	• Security (as per CCT policies)
	    o Authentication
	    o Single Sign-on
	• The Internet (Web Services)

Normalization of Data and Data Share	Workflow interactions should include: • Support the normalization of data within the various systems inside and outside of a UWL business unit utilizing workflow. o Token data elements should be normalized across systems within the workflow handoff. It should contain the required elements for sharing.

Core Functional Requirement Category	Core Functional Requirement
	• Facilitate token metadata share within workflow systems. • System verification of required approvals, data elements, etc. across multiple systems. • Data retrieval for display within workflow or application • Data retrieval for business rules processing of workflow, notifications, and display restrictions on the presentation layer.
Technical Constraints	The Workflow system must allow for integration with other systems, business applications and workflows. • CCT systems and business applications will change over the next few years and might be implemented upon various technology frameworks. This environment should be supported.

13.4.2.7 SEARCH ENGINE

A search engine would be required as part of the Document Management and Record Management solution. The search function needs to provide a single interface to perform search requests across the Document, Record and Case management repositories subject to the access and privilege rights of the users.

The requirements below are in addition to any search requirements stated under the various section under the section search and retrieval.

Core Functional Requirement Category	Functional Requirement – Search Engine

Functionality
The search function needs to provide a single interface to perform search requests across the Document, Record and Case management repositories, as well as other enterprise repositories if required, subject to the access and privilege rights of the users.
	Control
	• The search engine must be able to search for and retrieve a complete electronic folder, or folder part, and all its entries, and display all, and only, those entries in the context of that folder as a discrete group and a single retrieval process.).
	• The search engine must be able to search for, retrieve and display a set of electronic records taken from many different folders by specifying values to be searched for in electronic record metadata.
	• The search engine must be able to search for, retrieve and display an electronic folder by all implemented naming principles, including:
	    o a folder title text
	    o a folder numerical reference code.
	• Where full-text retrieval of record content is available, the search engine must ensure that a user who is not allowed access to an electronic record or folder cannot receive any information about the record or folder as a result of a full-text search.
	• When a search is completed, the solution identifies the latest version of the record, but all versions of the record are available for the user to select and view if have they the appropriate access rights.
	• Support a mix of metadata and content searches using controlled lists and combining search terms to conduct simple keyword and complex searches, using search terms such as Boolean terms, logical operators, broader and narrower terms, and proximity searches, as required.
	• The solution provides a help function to give guidance on searching and searching hints.
	• Retrieve information by searching the database using at least the following parameters:
	    o Full text;
	    o Combined text and field;
	    o Keyword;
	    o File/document;
	    o Metadata field;
	    o Date document created/captured;
	    o Author of the document;
	    o Barcode;

Core Functional Requirement Category	Functional Requirement – Search Engine
	○ Location; and ○ Classification scheme. • The solution retrieves information by searching across multiple databases, across all fields, from a single point of access, using the following minimum search functions: ○ Full text ○ Record format ○ Last action ○ Disposal action ○ Disposition (status) of record, i.e., active, inactive, destroyed, archived, transferred ○ Combined text and field ○ Keyword ○ Storage unit and record title and number ○ Dates e.g., records created, captured, destroyed, etc. ○ Author of record ○ Barcode ○ Location ○ Classification scheme ○ Unique identifier and ○ Metadata element. • The search engine should allow the user to refine search criteria and results at a user level, based on operational needs.
	Advanced Search and retrieval There are instances where it may be necessary to retrieve electronic records by content and to employ more sophisticated searching mechanisms to do so, including the use of a standard thesaurus. ○ The search engine must allow a RM Systems Administrator to specify any element of record and folder metadata, and optionally full record content, that is to be indexed for future retrieval, and to define stop lists and must support the ability to change this configuration at a later date. ○ The search engine must be able to retrieve electronic records and electronic folders by an integrated search mechanism on both record content, and record and folder metadata. ○ The search engine must provide search mechanisms that offer both a browsing or graphical navigation approach within the folder structure and a direct searching approach. ○ The search engine must provide Boolean and probability-based full-text search and retrieval mechanisms and relevance ranking of retrieval results ○ The search engine must provide user assistance by query formulation, including the use of a controlled vocabulary system. ○ The search engine must support the sorting, printing and saving of search results in variable display formats. ○ Where (non-record) electronic documents are managed alongside electronic records in the same system, the search engine must be able to search for and retrieve both documents and records in an integrated manner. ○ The search engine must ensure that all retrieval operations are consistent with all access control restrictions so that an unauthorised user cannot access folders or records by use of an advanced search and retrieval mechanism. ○ The search engine should allow search requests to be made from outside the system, and support the ability to exchange search requests and search results with other systems ○ The search engine must allow users to save and re-use search parameters within the system against their user or team names.

Core Functional Requirement Category	Functional Requirement – Search Engine

Indexing Customization
Most indices can be customized to better meet specific searching needs
	• Custom setup preferences must include:
	   ○ the sensitivity of upper- and lower-case letters,
	   ○ recognition of specific date formats,
	   ○ the inclusion or exclusion of specific file types, and
	   ○ Unicode compliance to identify and index foreign characters.
	• The inclusion of punctuation as a search operator, however, does not impact how a document is indexed. Derivations of a root term can also be queried by adding other characters such as asterisks, exclamation points and percentage signs. For example, a search for legal* would generate hits for legal, as well as legality, legalities, legalize, etc. Another example would be the addition of a tilde to the end of a word to search for all synonyms of that word.
	• The system should be able to search utilising multi-language ability to cater to the needs of South Africa.
	• The search engine needs to take the text in a document or record and break the text into searchable keywords through the process known as tokenization.
	• The system must support a free-text search that allows users to search every word in an entire document or a specified group of documents.
	• The solution must enable the RM System Administrator to configure default search options for end-users.
	• The solution enables the System Administrator to configure default search options for end-users.

User Access	• The solution must allow the RM System Administrator or accredited RM practitioner to search within the disposal schedule. • The solution must withhold all or part of a search result, according to user access privileges and information security classification.

13.4.2.8 PUBLISH

This module must cater for two scenarios. If the specified modules in this tender do not fulfil the requirement, then additional modules will have to be provided and declared in this tender response.

Scenario 1: CCT has many projects and other engagements with external stakeholders that require document collaboration. CCT provide access rights to a SharePoint site or folder or document to external parties. The external parties register users by using their private/company email addresses. Private e-mails belong to councillors of the CCT. The site/folder/document owner provide them with access. In the to-be environment as defined in this tender, the access will be required in the DMS under the auspices of the System Administrator.

Scenario 2: The second use case is the capability of CCT employees to access documents without having to be logged on to the network. Thus, if there is a link/URL embedded in an email, the employee can click on the link and access the document from any CCT owned device without having to be logged on to the network, provided that the employee has access to the document. The system must be able to create and provide the document URL or any other identifier that are hyperlinked to the document, so that it can be pasted or forwarded to the employees.

Functional Requirement Category	Functional requirement - Publish
Access to external parties *The system must be able to manage access and the*	Access to the RM&DM&CM system will be initially managed by the IS&T authentication and access procedures and systems. Once the user is allowed to access the RM&DM&CM environment, then: • The System Administrator or authorised user must assist in ○ registering the user or third party as a user on the RM&DM&CM solution.

Functional Requirement Category	Functional requirement - Publish
activities of third parties which have been subjected to online security procedures, and ensure that such processes do not impair the ability of the system to meet the core requirements of this specification.	o Create user profiles that will govern the access rights of the user of third party. • The Access and security functionality as defined in the EDMS, RMS and CMS must be adhered too.
Access to Employees with URL *The system must provide the ability for CCT staff to access documents via a URL or similar hyperlink object once the IS&T authentication and access have been granted*	Access to the RM&DM&CM system will be initially managed by the IS&T authentication and access procedures and systems. Once the CCT staff member has logged into the CCT environment then the user will be allowed to access the RM&DM&CM environment. then: • The system should allow the CCT staff member that has been provided with a document URL or hyperlink to automatically display the document that are referenced by the URL or Hyperlink. • The access rights of the user still need to be enforced and access must be blocked to a user if they do not have the right to view a document even if they have a hyperlink or URL. • The Access and security functionality as defined in the EDMS, RMS and CMS must be adhered too.
Creation of URL or document related hyperlink *The system must provide the users with the ability to copy a URL or hyperlink and forward the said link to a CCT staff member that will then be able to access the document via the URL or hyperlink subject to access rights and privileges*	The RM&DM&CM system must be capable of creating a document URL or hyperlink that can be utilised by users that have access rights to the RM&DM&CM system to view the linked document on any device logged into the CCT environment. The system must: • Provide the user with the document URL or hyperlink that allow users to access the artefact directly without having to engage in search actions. • Provide the functionality for the document URL or hyperlink to be forwarded via e-mail from the RM&DM&CM system to any user that have access rights in the RM&DM&CM system.

13.4.2.9 ADDITIONAL FUNCTIONAL REQUIREMENTS

Below is a list of additional functional optional requirements that would be beneficial to the CCT to ensure full compliance with regulations. These functions are usually catered for within the ICT operations. Failing the provision of these requirements as a standard ICT offering, then the system must be able to comply with these requirements.

The CCT have expressed their interest in utilising the RM&DM&CM workflow engine as an Enterprise solution if the said facility is capable of fulfilling this requirement. If not, do not incorporate an enterprise-wide workflow solution into this quote.

These additional primary functions include:
- Online security
- Workflow
- Hybrid system management

Additional Functional Requirement Category	Additional Functional requirement

Online security
 	
The system must be able to manage digital records which have been subjected to online security procedures, and ensure that such processes do not impair the ability of the system to meet the core requirements of this specification.
	Encryption
	• The system must be able to capture and register an encrypted record directly from an application capable of encryption.
	• The system must be able to store digital records in either encrypted or unencrypted form.
	• The system must support the use of metadata for digital records transmitted or captured in encrypted form, following the Recordkeeping Metadata Standard, including:
	   ○ the serial number or unique identifier of a digital certificate (where relevant);
	   ○ type of algorithm and level of encryption; and
	   ○ date and time stamps relating to encryption and/or decryption process.
	• The system must ensure that an encrypted record can only be accessed by those users associated with the relevant cryptographic key, in addition to other access controls allocated to the record.
	• The system must allow encryption and decryption when a record is captured or registered directly from another application.

	Digital signatures
	• The system must be able to interface with digital signature technologies so that authentication metadata can be captured automatically.
	• The system must be able to check the validity of a digital signature at the time of registering a digital record.
	• The system must be able to store with the digital record:
	   ○ the digital signature associated with that record;
	   ○ the digital certificate authenticating the signature; and
	   ○ any other confirmation details, in such a way that they can be retrieved with the record, but without compromising the integrity of a private key.
	• The system must support the use of metadata for digital records transmitted or captured bearing digital signatures, following the Record and Document Management Metadata Standard. At a minimum, this metadata must note that a digital signature was authenticated.
	• The system must allow a RM System Administrator to configure the extent to which authentication metadata is routinely stored with the digital record. For example:
	   ○ retain the fact of successful authentication only;
	   ○ retain metadata about the authentication process; and
	   ○ retain all authentication metadata, including signatures.
	• The system must be able to demonstrate the continued integrity of a digitally signed record, irrespective of whether authorised changes have been made to its metadata.
	• During an export process, the system should be able to apply a digital signature to:
	   ○ a digital record; and/or

Additional Functional Requirement Category	Additional Functional requirement
	o a digital folder containing multiple records, in a manner that supports external authentication.

	Authentication
	• The system must be able to store metadata about the process of authentication, including:
	  o the serial number or unique identifier of the digital certificate;
	  o the Registration and Certification Authority responsible for authentication; and
	  o the date and time of authentication.
	• The system must allow a configuration option to store authentication metadata:
	  o with the digital record to which it relates; or
	  o closely but separately linked to the digital record.
	• The system must be able to interface with PKI-based security technologies.

	Cryptographic key management • The system must support the implementation of a key management plan. • The system must be able to maintain cryptographic keys for the life of the record with which they are associated. • The system must support the separate, secure storage of encrypted records and their associated decryption keys. • The system must be able to store digital certificates for encrypted records and digitally signed records and must warn a RM System Administrator of any certificates approaching expiry. • The system must automatically record the details of all online security processes in an audit trail. • The system must support date and time stamping for all records subject to online security processes.

	Digital watermarks
	• The system must be able to store records bearing digital watermarks.
	• The system must be able to store metadata about a digital watermark:
	  o with the digital record to which it relates; or
	  o closely but separately linked to the digital record.

Workflow *The system may provide or be integrated with a workflow facility to support business and records management tasks in a controlled manner. The system must ensure that such processes do not impair its ability to meet the core requirements of this specification.* *Please note the request of the CCT IS&T division for the possible use of the*	**Workflow features** The system must have an enterprise-wide workflow capability that • must support workflows that consist of several procedural steps. • must allow standard workflows to be defined and maintained by a RM System Administrator. • not limit the number of steps for any given workflow. • must restrict the amendment of pre-programmed workflows to a RM System Administrator or other authorised user. • must record all changes to pre-programmed workflows in the audit trail. • must recognise both users and workgroups as participants. • must alert a user when a digital record has been sent to their in-tray for attention, and specify the attention required. • must support integration with electronic messaging facilities to notify users of records that may be waiting for their attention. • must track the progress of a digital record or physical file through a workflow, so a user can determine its status in the process. • should provide the functionality for the automation of documentation-intensive business processes, including document handling, storage, manual entries as well as

Additional Functional Requirement Category	Additional Functional requirement
RM&DM&CM workflow function to be utilised with other core applications. It does not form part of this section.	the verification of data to reduce time and resource wastage in performing manual indexing and verifications.
	Workflow management The system must have an enterprise-wide workflow capability that • must not limit the number of workflows that can be defined. • must provide comprehensive reporting facilities to allow the monitoring of volumes, performance, and exceptions. • should provide workflow capabilities to manage case, document, record-centric workflows, including origination, maker-checker, approval, and rejection.
	Workflow and records management The system must have an enterprise-wide workflow capability that ▪ must ensure digital records and folders remain correctly classified during a workflow process, retaining all links to other record plan entities. • must allow a digital document to be captured and registered during, or after, a workflow process. • must maintain the same access and security controls that apply to digital records and physical files at all other times. • must ensure that workflow processes do not interfere with the scheduled disposal of digital records and physical files. • must notify a RM System Administrator that a digital record or physical file within a workflow process is due for disposal. • must ensure that digital records and physical files within the workflow process can be located using the standard search interface. • must support the progressive addition of metadata to digital records and physical files, as set out in the Record and Document Metadata Standards.
Hybrid system management *The system must support the management of markers, physical folders and hybrid-folders in a manner consistent and fully integrated with the management of digital records and physical files.*	**Control and capture** • The system must support the management of markers, physical folders and hybrid folders in a manner consistent with the management of digital records and physical files. • The system must allow physical files to be classified with the same records classification tools in the same record plan used to manage digital folders. • The system must allow hybrid folders, which are part digital and part physical, to be classified with the same records classification tools in the same record plan used to manage digital folders. • The system must allow the physical and digital components of a hybrid folder to use the same title and unique identifier, but with appropriate indicators marking which is physical and which is digital. • The system must enable the creation of a marker for each physical record registered in the system. • The system must allow markers to denote different types of physical records, allowing a user to enter the format as descriptive metadata. • The system must allow markers to be classified with the same records classification tools in the same record plan used to manage digital records. • The system should provide various library functionalities, such as check-in, check-out, auto-versioning, etc. • The system should provide the users with the ability to add notes and comments on cases, documents, records and folders for the users to collaborate on content seamlessly within the system.

Additional Functional Requirement Category	Additional Functional requirement
	Access and security • The system must ensure that the physical and digital components of a hybrid folder are allocated the same access and security controls. • The system must maintain the same access and security controls for markers, physical folders and hybrid folders that apply to digital records and folders at all times.
	Disposal • The system must support the application of a disposal class to a physical folder, in a manner consistent with the management of digital folders. • The system must ensure that the physical and digital components of a hybrid folder are allocated the same disposal class. • The system must ensure that the disposal action carried out on a hybrid folder is applied to both physical and digital components at the same time, taking into account the different processes required for destruction where applicable. • The system must apply disposal review decisions to both the physical and digital components of a hybrid folder. • The system must ensure that destruction or transfer of digital folder results in the destruction of any markers contained in that folder. • The system must maintain minimum metadata for destroyed items, including markers, physical folders and hybrid folders. • The system must alert the RM System Administrator to the existence and location of the physical component of a hybrid folder when such a folder is due for export or transfer. • The system must allow the export of physical folders and hybrid folders, retaining all associations with the digital component of the hybrid folder and the record plan once they are exported. • The system must allow the export of markers, retaining all associations with digital records and folders once they are exported. • The system must require a RM System Administrator to confirm that the physical component of a hybrid folder has been transferred, exported or destroyed before the digital component of the folder can be processed.
	Searching and retrieval • The system must be able to retrieve markers, physical folders and hybrid folders along with digital records and folders, using the same search interface. • The system must ensure that retrieval of a digital folder also retrieves all markers associated with that folder. • The system must ensure that when a hybrid folder is retrieved, its physical and digital components are also retrieved.
	Metadata • The system must support the use of metadata for markers, physical folders and hybrid folders, including inheritance of metadata consistent with inheritance by a digital record or folder. • The system must allow a different metadata element set to be configured for markers, physical folders and hybrid folders than that for digital records and folders so that metadata for physical entities can include physical location information. • The system must record changes to location metadata in the audit trail.
	Scanning • The system should provide for the conversion of paper-based documentation to be digitised from a centralised or decentralised high-volume environment subject to the

Additional Functional Requirement Category	Additional Functional requirement
	scanning strategy of the CCT. The conversion should allow for full text indexing and full text search of the documents by means of optical character recognition (OCR). • The system should provide for fast conversion of high volumes and ensure quality of data is maintained • The system should be capable of identifying first and last pages by means of a barcode reader in a batch of documents to eliminate manual actions required to add or remove separator pages and have the ability to combine, separate, modify and import documents when required. • The system should provide for the automatic classification of documents imported in bulk. OCR and/or other similar technology should be utilised to read the text of documents and classify the document into metadata categories based on the information retrieved. • The system should provide Image enhancement technologies and techniques to ensure quality scanned images thereby reducing the need to rescan paper-based objects due to poor original quality results. • The system should allow for seamless integration with the workflow engine as per business requirements and ensure the document is captured in the DMS or stored as a record in the RMS with the appropriate metadata • The system should automatically read, index and extract data from documents and barcodes, irrespective of type and format • These requirements should be fulfilled in line with CCT security protocols as well as standards and legislation that applies. • .

13.4.3 NON-FUNCTIONAL REQUIREMENTS

The ISO/IEC 25010 standard offers us a product quality evaluation system with a reasonably rigorous classification for NFR's. A non-functional requirement (NFR) specifies how a component should perform. NFRs define the desired qualities and rules of conduct in the ecosystem, whereas functional requirements define the vehicles for functional delivery.

They are used to describe key operational characteristics of the components and services that make up the CCT's RM&DM&CM platform, rather than specific behaviours.

The requirements listed below will either be provided by the RM&DM&CM solution or controlled and provided by another service within the IT landscape, for example, single sign-on logically fits within the access provisioning of ICT whilst a single user-GUI to access all the modules of the RM&DM&CM system is a non-functional requirement that usually is fulfilled by the RM&DM&CM solution.

The solution should be easily scaled up to work for a Multi-location environment that might require replicating Image Servers and load-balancing Web Servers. A required document management system should have easy to use XML API's and Web-Services interfaces to facilitate integration with other business systems like Workflow, Records Management, and Image Enabling of ERP & CRM applications, Core Insurance & Banking applications.

For clarity, the NFRs are used to describe qualities that are observable during execution such as performance, accessibility, and usability characteristics; and qualities that describe how the ecosystem develops, such as testability, maintainability, extensibility and scalability, which are vital for a platform to be dynamic, and evolve.

Non-Functionality Category	Non-Functional Requirements
Security (*Degree to which a system protects artefacts, information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization*)	• Login / Access levels – The user configuration within the system should fulfil this NFR. • Create, Read, Update, and Delete (CRUD) levels - The user configuration within the system should fulfil this NFR. • Access permissions for application data may only be changed by the system's administrator and full audit traceability must be provided by the system reflecting all such interactions. • Separation of duties – the system should enforce the separation of duties of all security actions and processes involving independent actioner and approver roles. Due to the legal, governance and compliance requirements linked to Content management, the following NFR must be controlled by the system and not the general ICT policies: • Inactivity timeouts –the timeout durations, actions, and traceability requirements • System data backed up every *x* hours and copies stored in a secure off-site location. • Encryption (data in flight and at rest) – All external communications between the system's data server and clients must be encrypted and comply with the standards and regulations of the record management oversight agency. To comply with legislation and regulations, the system must satisfy the following requirements: • Confidentiality - Degree to which the system ensures that cases, documents, and records are accessible only to those authorized to have access. • Integrity - Degree to which the system and components prevent unauthorized access to, or modification of artefacts or data. • Non-repudiation - Degree to which actions or events can be proven to have taken place so that the events or actions cannot be repudiated later. • Accountability - Degree to which the actions of an entity can be traced uniquely to the entity. • Authenticity - Degree to which the identity of a subject or resource can be proved to be the one claimed. Required software and system must have Industry-strength Security with the following features & functionalities. • Definition of Users and Groups in the system • Access permissions on Folders, documents, and Data Classes • Multiple levels of access rights (Delete/Edit/View/None) • Grant users' privilege of creating users and groups

Non-Functionality Category	Non-Functional Requirements
	• Secure login and passwords for each user • LDAP authentication and single sign-on support • Support for Data and Password Encryption • Support for Digital Signatures and Biometric integration if these functions are not modules within the system but rather 3rd party add-ons • Supports SSL/HTTPS for secure transmission (Only TLS 1.2 or later supported as per cryptographic SOP)
Audit (*Define the level of traceability for transactions required*)	• The system must maintain full traceability of transactions • User and transactional interactions must be time and date stamped by the system
Capacity (*Provisioning for growth*)	• Throughput – the system must be able to handle 100000 transactions per hour as defined by the volume requirements during transactions peak times • Storage – (memory/disk) – the volume of data the system will page/persist at run time to disk • Year-on-year growth requirements (users, processing & storage) 30%
Performance **(**The accomplishment of a given task measured against pre-set known standards of accuracy, completeness, cost, and speed.)	• Response times – Remote sites need to load, display and save documents and information within a variance of 25% than the times recorded at CCT HQ. • Processing times – functions, calculations, imports, exports • Bandwidth requirement – Due to cost to provide high-speed bandwidth connectivity, the response time and processing time NFR's must be accomplished with the minimal and not maximum bandwidth. • System automation – the system should auto-create and apply the appropriate taxonomy, file structure and archiving rules where possible to minimise human intervention. • Interoperability - The system must provide the ability to move information and artefacts easily between people, organisations and systems by providing standard API's to ERP, and productivity packages. It is imperative that when information is shared between people and systems, its meaning is preserved from one context to another so that information is interpreted in the same way. That is, what was meant is the same as what is understood. This is the concept of "semantic" interoperability, which can be defined as: "The capability of two or more systems to communicate and exchange information, and for each system to be able to interpret the meaning of received information and to use it seamlessly with other data held by that system"
Availability (*Uptime - Refers to the percentage of time that the infrastructure, system or a solution remains operational under normal circumstances to serve its intended purpose*)	• Operational availability – the system must be available during the hours of operation as well as the days as required by business that might differ from the standard IS&T availability policy. This would require the system to control these parameters independent from ICT. • Locality – the operational availability might differ from regional offices to HQ and the system should support site-specific availability parameters. • Replication – the system should support replication between remote or local Image Servers in the case where a cloud solution is not deployed.
Object integrity (the overall accuracy, completeness, and consistency of data and objects)	• Data, artefacts, and information Integrity – the system should have the ability to ensure consistency of events, values, methods, measures, expectations and outcomes across data, artefacts, and information. • Compliance to data and information protection laws –the ability to apply and govern the application of compliance with, relevant information management regulation such as GDPR, POPIA. • Database recovery – the ability of the system to rebuild a consistent point in time set of data for the operating environment primarily for databases, but also for unstructured and configuration data sets.

Non-Functionality Category	Non-Functional Requirements
	• Mean Time to Recovery – if broken, how much time is required to get the system back up again.
Total Cost of Ownership (TCO) (an estimate of all the direct and indirect costs involved in acquiring and operating a system over a period)	• Reduced TCO by leveraging existing IT infrastructure - Products should be available on all industry-standard Operating Systems, Databases and Application Servers, and should be deployed on the platform of choice of the customer. Products should also be deployed on open-source platforms.
Usability (Degree to which a product or system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use)	• User Standards (**Look / Feel**) – Menu that provides access to all modules with the same look and feeling complying with Internationalization spellings, keyboards, etc. requirements • User error protection. The system needs to enforce data integrity, duplicate record validation, etc. to ensure that the system protects users against making errors. • Personalisation – the ability of the system to facilitate individual preferences to be recorded and employed in all interactions without repeated user selection of preferences
Resourcing (the reliance of the customer on software expertise to configure, customise or provide ongoing support)	• Ease of installation – Refers to the ability to install and configure the system by the customer's resources • Available resource – the availability of expert resources with their associated labour factor to successfully deploy the system • Continuous reliance on external support –to reduce the reliance on external parties, what is the cost and effort required to power the internal resources of the CCT to manage and support the system
Documentation	• The availability and completeness of User Documentation • System Documentation to enable the CCT's technical staff to provide 1st line support function • Help? – the provision of a system integrated or online self-help facility • Training Material – complete and ease-of-use of materials for a user to refresh their knowledge or for new staff to familiarise themselves with the system.
Disaster Recovery functionality	Required software and system must have Disaster Recovery functionality with the following features and functionalities: • Support for backing up and restoring of information for disaster recovery • Support for incremental and full Backups • Support for replicating data onto remote sites
Third-Party Integration A comprehensive set of API's and SDK's should be available which should be used for unleashing the full power of both Business process management and document management system.	• The required solution should be component-based and can be deployed independently of each other by integration with any third-party core business application. • A comprehensive set of API's and SDK's should be available which can be used for unleashing the full power of the BPM and ECM / RM&DM&CM both. • Out of the box (OOTB) configuration using predesigned, pre-packaged templates, forms, workflows that in place. • OOTB configuration time period to be 4-6 weeks • Should the RM&DM&CM solution require Open JDK for JAVA runtime, all costs and technical requirements should be catered for by the SI
Platform-independent DMS Web version	Required system and software should have Platform-independent DMS Web version • Required system and software should Expose standard Document Management features through a web interface • Required system and software should Use XML interfaces to internally communicate with the Transaction Server

Non-Functionality Category	Non-Functional Requirements
	• Required system and software should be available on Windows, Linux and UNIX platforms. • Browser support for the latest version supported by the CCT Edge Chromium

13.4.4 CCT's INTEGRATION GUIDELINES

As indicated in the tender, the Document and Records Management solution will be implemented in an environment where the ecosystem will change over a few years. This would require that workflows and system integration will have to be amended until the environment is finalised.

However, over the lifetime of the RM&DM&CM solution, it is anticipated that some systems would be replaced for whatever reason.

The RM&DM&CM vendors will be responsible for workflow changes and or integration changes resulting from these system changes.

The selection of an enterprise software solution to manage system integrations will run in parallel with the RM&DM&CM tender. However, the principles and guidelines for system integration will be guided by the integration guidelines and principles as listed below. The RM&DM&CM vendors need to ensure that they and their software are capable to comply with these guidelines and principles.

Technology Supported (Refer to paragraph 2.2.1.1.6 of the Eligibility Criteria and paragraph 13.5.1 of Technical Requirements)
The RM&DM&CM Solution should support modern technology based on table provided as a minimum. The Tenderer to complete **Schedule 15I – Technical Requirements: Technology Supported and** must indicate in the column "Compliant Yes / No" whether the proposed solution adhere or can deliver on the specified technical requirement. Where the proposed solution doesn't meet the requirement or partially meets the requirement, the Tenderer must clearly indicate which functional requirements cannot be delivered on and provide a response or explanation how this situation can be mitigated. The Bid Evaluation Committee will assess whether the mitigation/ solution provided conforms to the scope required. The Tenderer can also add relevant information as an annexure to the tender response with a clear reference to the item the information refers to. Please refer to clause 2.3.7. Test for responsiveness on this matter.

PARADIGM/ CONTEXT	PROTOCOLS	SERIALISATION/ DATA FORMATS
File Transfer	FTP (IETF Datatracker RFC959)	
ODBC		
Email	POP3 (IETF Datatracker - RFC1939) SMTP (IETF Datatracker - RFC5321) IMAP (IETF Datatracker - RFC3501) COAP (IETF Datatracker - RFC7252)	
REST SOAP	HTTP/1 (IETF Datatracker - RFC7230)	JSON (IETF Datatracker - RFC8259) XML (W3 - Version 1.0, 1.1)

	HTTP/2 (IETF Datatracker - RFC7540) HTTP/3 (draft-ietf-quic-http-34) WebSockets (RFC6455)	YAML (YAML - Version 1.2)
Message Queue Pub-Sub	Kafka Protocol AMQP (AMQP - 1.0, 0-9-1) ZMTP (RFC.ZeroMQ - 23/ZMTP) MQTT (OASIS - Version 5)	

13.4.5 PILOT SCOPE AND IMPLEMENTATION

It will be expected from the winning bidder to prove to the CCT that the solution he/she provides is capable of delivering on the requirements of the CCT. **Refer to Section 7 point 37 under Special Conditions of Contract.** This will be done by means of a pilot project that will include all functionality of the solution to be tested on legacy systems chosen by the IS & T department of the CCT. Testing criteria will be set up by CCT IS & T Officials and measured accordingly. If the bidder's solution does not meet the minimum expected results, the award will be offered to the bidder that is next on the evaluation list conducted by the CCT.

SCOPE

- To test the capability of the tenderer to successfully configure the identified applications and migrate the content of these applications to the target solution.
- To successfully integrate the applications with legacy systems.
- The pilot consists of various phases based on options provided.
- All phases will need to be successfully completed within the specified time period in order to move on with the implementation.
- The test cases chosen will consist of SharePoint (SP) and SAP Records and Case Management (RCM) solutions with a sufficient amount of complexity to test the capabilities of the tenderer within the specified pilot time period.
- In parallel with the pilot, the tenderer must do a full analysis and provide a report on the Development Application Management System (DAMS) to identify if this solution can be configured in RM&DM&CM or whether extensive customisation is required.

Measures of Success and Dimensions to be evaluated:

Dimension	Deliverable	Measure of Success
1. **Pilot Planning**	1. Detailed pilot implementation plan including migration strategy and cleansing proposal	1. Signed off implementation plan
2. **Content**	2. Transaction report detailing volumes pre and post migration 3. Metadata proposed and assigned to documents	2. 100% of data migrated 3. 100 % of metadata assigned – verified by business
3. **Functionality**	4. Functional specifications – including build of file classification systems 5. User acceptance documents	4. Functional specifications signed off by IS&T

			5. User acceptance signed off by business
4. Access and Permissions	6. Report detailing permissions prior and post migration – staff who have left the organisation should be removed		6. User acceptance signed off by business
5. Training and change management	7. Initial end user, power/super user and system admin training content delivered 8. Training delivered 9. Seamless transition from old environment to new 10. Documented lessons learnt to be utilized for the rest of the implementation		7. Training content signed off by respective owners 8. No. of staff trained and certified
6. Quality Gate Assessment	11. Dimensions 2, 3 and 4 must be completed for each of the Pilot deliverables		9. 90% of dimensions 2, 3 and 4 is the minimum requirement for success in each phase. 10. In order to move from Pilot 1 to Pilot 2, 90% of successfully completing Pilot 1 is required. 11. The remaining 10%, if applicable, must be completed within that specific Pilot group. If the 10% is still outstanding at the end of that Pilot group then the CCT reserves the right to find the service provider non-compliant and consider this a fail.

Table 6: Dimensions to be measured during pilot period

Details of the pilot cases:

The CCT requires 3 pilots to be completed over the 6 month period allocated for the pilots. Each pilot will consist of phases and each phase will be measured based on the successful completion of the applications/sites/solutions which have been identified for that specific phase. The review and analysis of DAMS is also required and will run in parallel with the pilot cases.

It is envisioned that the initial 3 months prior to the commencement of the pilot will be utilised for the installation and configuration of the RM&DM&CM solution as well as analysis and design work so that a detailed implementation plan can be developed by the bidder and signed off by the CCT prior to the start of the pilot.

The following tables represent a breakdown of the pilots and the applications/sites/solutions required to be implemented in the specific phase. The applications/sites/solutions have also been assigned a category (A/B/C/D) which has been utilised to classify the applications/sites/solutions into high level functionality and complexity. More detail regarding the categories are available in section **13.5.6.1 Functional categories for SharePoint, SAP RCM and FS01**, Table 8.

Pilot 1:
Phase 1:

Solutions	Type	Category	Volume
10 MySites	SharePoint Site	A	0.17TB
20 TeamSites			4.94TB

Solutions	Type	Category	List Count	Total Items count	Site User Count	Workflows per solution
City Manager Mail Tracking System	SharePoint CTApp	B	43	781	19	1

Phase 2:

Solutions	Type	Category	Sub-processes	No. of files	Workflow packages	Integrations
Agreements	SAP – Records Management	C	7	112 332	0	3
Contract Management	SAP – Records Management	C	4	22 868	0	1

Pilot 2:
Phase 1:

Solutions	Type	Category	List Count	Total Items count	Site User Count	Workflows per solution	Integration
ID Card Application	SharePoint CTApp	C	50	23 093	8 125	39	Yes
Council Decision Implementation Tool	SharePoint CTApp	C	49	4 394	674	17	Yes

Phase 2:

Solutions	Type	Category	Sub-processes	No. of files	Workflow packages	Integrations
Property and Real Estate	SAP – Records Management	C	8	26 239	0	13
Revenue Collection	SAP – Case Management	D	1	770674	0	0

Pilot 3:
Phase 1:

Solutions	Type	Category	Sub-processes	No. of files	Workflow packages	Integrations
Water Pollution Control	SAP – Case Management	D	4	38 185	2	0
Social Development & Early Childhood Development	SAP – Case Management	D	8	156	1	2

Review and Analysis of DAMS:

The CCT also requires the DAMS solution to be analysed and a technical report delivered to describe how the DAMS functionality will be developed in the RM & DM solution. DAMS is a highly customised solution that consists of different functionality, a major part being case management. The purpose of the report will be to advise on how much of DAMS can be configured in the RM & DM solution versus the how much customization may be required. The delivery of this report will run in parallel with the pilot cases described above.

Solutions	Type	Category	Sub-processes	No. of files	Workflow packages	Integrations
Development Application Management System	SAP – Case Management	D	4	8 388 032	102	95

The below table represents a summary and sequencing of the pilot cases to be completed.
It should be noted that the CCT landscape is evolving and that if the below pilot cases are for any reason removed from the pilot, the CCT reserves the right to select cases of a similar complexity:
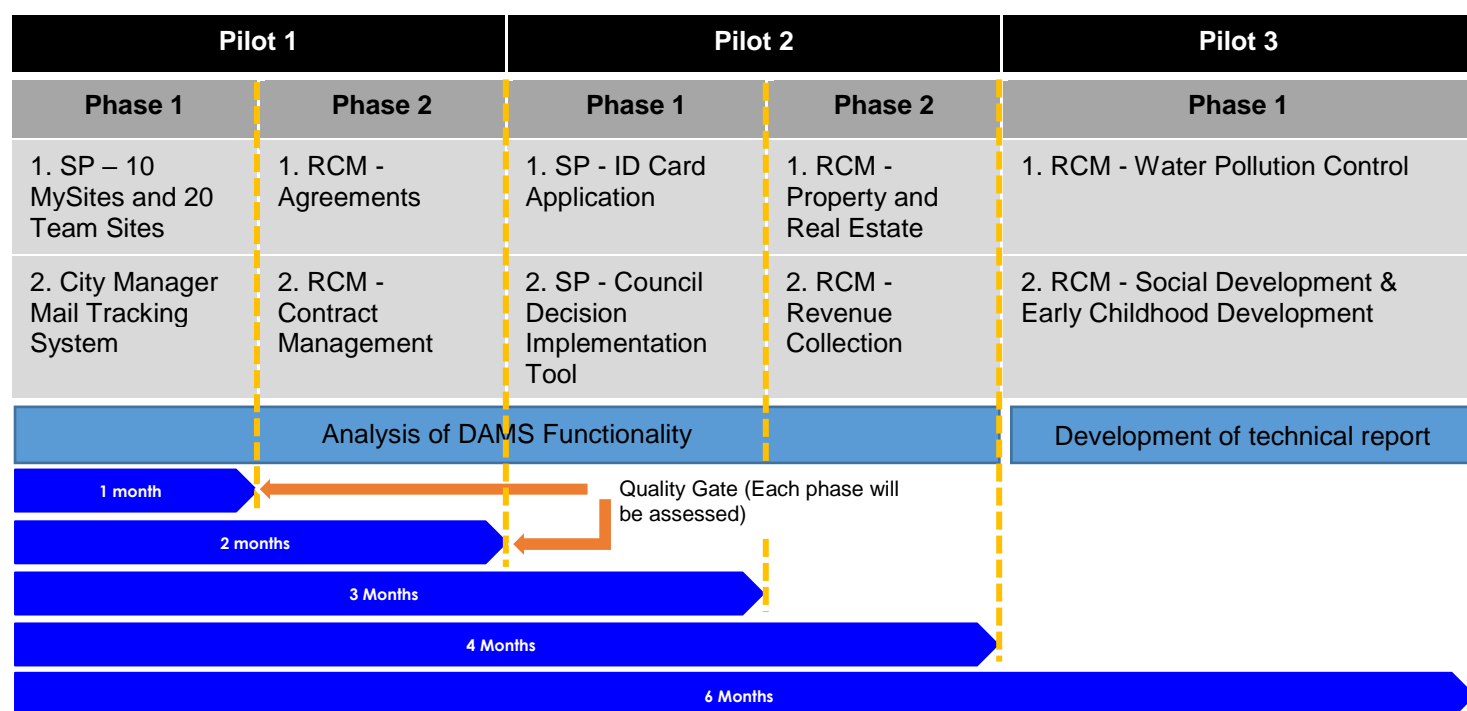
Figure 5: Three pilots, 10 solutions over 6 months and the analysis and review of DAMS

13.5   REQUIREMENTS FOR THE IMPLEMENTATION OF THE RM&DM&CM SOLUTION

Please note that a Detailed Project Plan to be provided in your response for the below deliverables in Schedule 15 J with a strong focus on migration, integration and development inclusive of methodology and approach.

The phases and deliverables identified here are aligned with the CCT Project Management Office methodology for implementation projects and tenderers are required to be familiarised with these requirements when responding to Schedules A to B

Minimum Requirements for a project plan:
- Include the following activities:
  - Discovery and Planning
  - Design
  - Development
  - Testing
  - Deployment
  - Migration, Integration and Development
  - Input into Change Management
  - Enhanced three-month period of support post Deployment
- Contain milestones
- Contain Stage gates per phase and minimum requirements to pass
- Provide RACI Matrix taking into account dependencies on CCT

Please respond to this requirement in **Schedule 15J** of the tender. The information provided will not be used for evaluation purposes.

13.5.1   Project Initiation Phase:

•   The Project Initiation phase begins with a Business or IS&T need; problem or opportunity being identified and the requirements thereof specified. These requirements are then communicated to IS&T, who evaluate the request for viability. The output documentation of this phase is a Project Initiation Document.

13.5.2   Project Planning Phase:

•   The Project Planning phase follows on from the approval of the project (Project Initiation phase) and involves the scoping of the project in more detail and the planning of the project tasks and activities needed to execute the project. This includes reaffirming the identified benefits and potential risks the project could encounter. The output documentation of this phase is a Project Charter document, Benefits Realisation Register, Risk Register and a Project Plan.

13.5.3   Project Execution Phase:

•   The Project Execution phase follows on from the Project Planning phase and involves the execution of the project plan and the management processes undertaken to monitor and control the deliverables of the project. Once all of the deliverables have been produced and the customer has accepted the final product, the project is ready for closure. The output documentation of this phase is Agenda's and Minutes of Meetings, Project Progress Reports, Project Change Requests, Risk Register, Issues Register and Benefits Realisation Register.

13.5.4   Project Closure Phase:

•   The Project Closure phase follows on from the Project Execution phase and involves the monitoring and support of the implemented solution in Production for an agreed period of time and the subsequent closure of the project. The output documentation of this phase is the Project Closure Report.

13.5.5   Post Project Review Phase:

•   The Post Project Review phase is an optional phase which follows on from the Project Closure phase at an agreed period of lapsed time and involves the measurement of the benefits, as determined in the benefits realisation register. The output documentation of this phase is the Updated Benefits Realisation Register.

13.5.6 Scope of implementation

The scope of the implementation takes into the account the current environment as outlined in Section 13.3 Current Architecture and Landscape. The table below indicates the scope and requirements of the implementation for the specified implementation period. It is important to note that the actual quantities depicted below will change by the time the implementation commences.

System	Type	Consists of	Volume	No. of Files	Workflows/Workflow Packages	Configure/ Develop	Migrate (metadata and documents)	Integrate
Custom Dev (.NET)	Custom	• Lists and workflows • Documents and records	Included in CTApps	Included in CTApps	N/A	N/A	N/A	7
SharePoint	CTApps	• OOTB functionality • Custom with OOTB functionality • Lists with workflows • Forms with workflows • Documents and records	Approx. 0.491TB	1 178 400	735	110	110	9
	MySites	• Lists • Images • Documents and records	6.2TB	8 061 776	0	17 700	17 700	N/A
	TeamSites External TeamSites		36.1TB	28 907 916	0	3200	3200	N/A
SAP RCM	PSRM (NXP)	• OOTB functionality • Custom with OOTB functionality • Forms with workflows • Cases and workflows • Documents and records	Approx. 20TB	33 811 818	206	30 solutions 160 sub processes	30 solutions 160 sub processes	363
	ECC6 Records and Case (RP1)							
SAP ECC6 Documents	ECC6 Modules	• OOTB functionality • Custom with	Approx. 40TB	To be identified during analysi	To be identified during analysis	To be identified during analysis	Approx. 40TB	To be identified during analysis

		OOTB functionality • Forms with workflows • Cases and workflows Documents and records		s				
ESRI	Spatial (EGIS)	N/A	N/A	N/A	N/A	N/A	N/A	2
File Server (FS01)	G: Drive	• GIS data and imagery • Audio and video • Databases and troubleshooting tools • Documents and records	Approx. 29.9TB	13 710 519	N/A	N/A	Approx. 29.9TB	N/A
	I: Drive	• Images and video	Approx. 11.8TB	1 337 755	N/A	N/A	11.8TB	N/A

Table 7: The figures in the table above indicate current volumes and will be confirmed during implementation of the solution

It is important to note the growth considerations, on the current stated data volumes, in this document for pricing in SCHEDULE C.   PROVISION   OF   ONCE-OFF   SERVICES   FOR   INSTALLATION IMPLEMENTATION AND MIGRATION OF THE RM&DM&CM SOLUTION

Estimated growth is 30% year on year on the stated volumes in this tender document– last volumes recorded in June 2022

13.5.6.1 Functional categories for SharePoint, SAP RCM and FS01

The application landscape that is in scope for the implementation includes a variety of applications and solutions that have been developed specifically on the SAP and SharePoint platforms. These solutions are utilised by business areas across the organisation and consist of functionality which varies in its complexity. The table below provides a high-level overview and estimation of the grouping of the key functionalities into categories from A to D, A being the least complex and D being the most complex. The specific in scope environments have also been listed below to indicate the categories in which the various solutions reside. An environment can have solutions that can be classified into either of the categories.

CATEGORY A	CATEGORY B	CATEGORY C	CATEGORY D
Out of Box		Custom Code	

No configured workflows	Workflows		
No integration		No to minor integration	Major integration
Manual upload		Manual upload and/or automated upload	Automated upload
			Case management
Lists/Libraries/Folders			
Data, Documents and records storage			
TeamSites, MySites, FS01, CTApps	**CTApps**	**CTApps, Custom Dev, SAP RCM**	**SAP RCM, EGIS**

Table 8: Functional Categories of existing applications/solutions

CTApps	Category A	Category B	Category C	Category D	Sub Totals
# of Apps	3	102	5		**110**
# of Lists	152	4993	261		**5406**
# of Items	4473	887 985	40 544		**933 002**

MySites	Category A	Category B	Category C	Category D	Sub Totals
# of Sites	17 700				**17 700**
# Files	8 061 776				8 061 776
Volume (in TB)	6.2TB				**6.2TB**

TeamSites	Category A	Category B	Category C	Category D	Sub Totals
# of Sites	3 200				**3 200**
# of Files	28 907 916				**28 907 916**
Volume (in TB)	36.1TB				**36.1TB**

FS01	Category A	Category B	Category C	Category D	Sub Totals
# of Files	15 048 274				15 048 274
Volume (in TB)	41.7TB				**41.7TB**

SAP RCM	Category A	Category B	Category C	Category D	Sub Totals
# of Solutions			15	15	**30**
# Files			13 650 037	20 161 781	**33 811 818**
Volume (in TB)			~8TB	~12TB	**20TB**

SAP ECC6	Category A	Category B	Category C	Category D	Sub Totals
# of Solutions					
# Files					
Volume (in TB)			40TB		**40TB**

The above categorisations are an estimate of the detail and complexities of the applications. The requirements and technical specifications for each application will be discovered through the actual project scoping of the implementation. The key activities envisioned for the implementation are set out

below:

Category	Requirement

Analysis and Design	• Engage with key stakeholders as identified by the CCT
	• Analysis of existing solutions and business requirements
	• Analysis of content of in scope environments to provide insights and recommendations i.e. scrubbing of data, metadata proposals and classification of records, disposal based on retention periods
	• Develop technical and project documentation as per CCT project methodology
	• Develop detailed implementation plan based on scope identified by CCT
	    o The implementation plan must take into account the CCTs evolving landscape and be sequenced accordingly
	    o FS01, SharePoint and SAP RCM development and migration must be completed during the implementation period
	    o SAP ECC6 data and content analysis, classification and migration

Development	• Configure/Develop all existing solutions as identified as in scope by the CCT • Configure/Develop all existing workflows of identified in scope applications • Configure/Develop the parts of existing custom built applications as identified as in scope

Migration	• Convert existing source schemas to target schemas
	• Resolve any issues identified during the conversion process
	    o Reports to be provided of success/failures
	• Cleansing of user access and permissions
	    o Removing access of staff no longer employed at the CCT
	• Migrate, and classify where necessary, all metadata and documents from identified source systems to target solution
	• Resolve any issues identified during the migration process
	    o Reports to be provided of success/failures
	• Provide disposal options based on retention periods

Integration	• Integrate the newly developed RM&DM&CM solutions with the legacy applications that were previously integrated • Integrate the newly developed RM&DM&CM solutions with the legacy SAP ECC6 modules generating records.
Training and change management	• Develop training material for end users of the RM&DM&CM system • Develop training material for administrators and support staff, power/super users of the RM&DM&CM system • Facilitate train the trainer, system admin, business admin and power/super user training sessions • Provide standard and best practice guidelines regarding the change intervention that will be required for this specific software solution • Input towards the updating of existing procedures and processes • Identification of new procedures and processes and contribution towards the development of this documentation
Implementation of pilot	• The pilot implementation is expected to cover all of the above-mentioned requirements

Table 9: Implementation requirements for identified scope of existing landscape

The following table show the envisaged timelines for the overall implementation. Tenderers need to incorporate these timelines in the definition of the detailed implementation plan as well indicate the resource allocations.

Category	Duration
Setup and Pilot	9 months
SAP Records and Case Management (including ESRI)	6 months
Microsoft SharePoint (including Custom Dev)	9 months
FS01	9 months

Table 10: Envisaged Timelines

Note: The above is an envisaged timeline but the expectation is that the tenderer provide an implementation timeline based on an interpretation of the requirements for the implementation and migration. The City reserves the right to negotiate the final terms and conditions of the overall implementation, including the implementation timelines and the commencement and completion dates for each category with the awarded Tenderer.

13.5.6.2 SPECIALISED TOOLS and RESOURCES
Refer to and complete Schedule 15L in Schedule 15 of Supporting Schedules

The SI to ensure that the project team is adequately staffed with **certified and highly skilled SAP and SharePoint resources.**

The SI must provide the necessary intelligent tools to conduct in-depth analysis of the SAP Records and Case Management (RCM), SAP ECC6, SharePoint and FS01 content. The tools must support high performance migration, automated file analysis, auto classification, tagging, need to be compliant, **and vendor approved for the SAP, SharePoint and FS01 environment.**

Reports must be generated that details amongst other Volume of Artifact types per Site Owner, Number of Artifacts, Age Analysis of Artifacts, Classification of Artifacts, End-to End Treatment of Artifacts, Metadata analysis, Active and Redundant Users, Compliance to SA Law re Record Management and Document Management as well as POPIA.

Item	Requirements	Applicable values
1.	**File Analysis** Perform analytics on content stored in unstructured and semi-structured environments.	• On-premise/Cloud • Must connect to SharePoint, SAP and Windows File Share services as a minimum • Must index and analyze high volumes (>100TB) of data and large files (>300MB) • Must not slow down performance of source systems • Must operate between 95% and 99.9% uptime • Must be able to process high volumes without impacting the performance of the tool • Must provide in depth and visual reports on usage and management of files and metadata which can be aggregated for summary reports
2.	**Data Classification** Perform analytics on content and assign/recommend metadata tags	• On premise/Cloud • Must connect to SharePoint, SAP and Windows File Share services as a minimum • Must index and analyze high volumes (>100TB) of data and large files (>300MB) • Must perform analysis of native metadata, custom metadata and file content to recommend metadata based on content of file • Must be able to manually amend metadata recommended • Must be able to automatically assign metadata to files as per automated recommendations or manual verifications
3.	**Data Migration** Perform data migration of metadata and documents from structured, semi-structured and unstructured environments	• On premise/Cloud • Automated • Must connect to SharePoint, SAP and Windows File Share services as a minimum • Must not slow down performance of source systems • Must operate between 95% and 99.9% uptime Must be able to process high volumes (>5TB per day) without impacting the performance of the tool • Must allow for schema identification and mapping from source to target • Must have built in data validation tools to report on migration success/errors

| | | • Must have reporting capabilities to provide automated and real time updates on migration processes |
| | | • Must allow for data to be transformed |

13.5.6.3 DECOMMISSIONING STRATEGY

The decommissioning strategy is intended to provide a standardised and holistic process for decommissioning applications within the City of Cape Town (CCT). This will require various departments, teams and processes to work in synergy to achieve results. The operationalisation of the decommissioning processes will need to be embedded in CCT project management methodologies and processes. Current application backup, archiving and restoration processes are critical in achieving successfully decommissioning status. IS&T projects that require migration of data to new target systems will require elements of decommissioning to be embedded into their associated project plans.

The City of Cape Town provides essential services to citizens and it has established highly effective support systems that enable delivery of these services. As business needs and technology continue to evolve, these support systems must also evolve in tandem with the business. As a result, obsolete and Legacy Systems are retired, or replaced, and decommissioned.

The high-level process for system decommissioning may require migration to a receiving/target system data, or business functions, that have been supported by a legacy system that is to be decommissioned. In this case, the transition requires a migration plan that should be established, and those migration tasks be completed before the legacy system is decommissioned. At the end of the migration process, accountable representatives should then sign a certificate of migration, acknowledging that all migration activities have been successfully performed. Once the certificate/document of migration has been signed, decommissioning plan development and subsequent decommissioning activities can be performed to terminate operations of the legacy system.

13. 6 REQUIREMENTS FOR TRAINING SERVICES ON THE RM&DM&CM SOLUTION

The following provide for the requirements and deliverables for training on the RM&DM&CM Solution. Refer to Schedule **E in section (5) Price Schedule**

Deliverable Category	Requirement Description
Train the Trainer	It is required to provide for the necessary support structure and resource capacity needs in order to run the RM&DM&CM solutions effectively through the training of CCT support staff. The train-the-trainer model is a training framework that turns employees into subject matter experts who can then teach other members of the organization. • A select number of employees will be trained as an internal trainer. • These trainers instruct and guide all other staff in the use of the software. • With the new RM&DM&CM system a number of so-called 'key users' must be trained. • Users must be from key business departments with excellent knowledge of the business processes who are able to transfer this knowledge to the other employees of their department as they will be the first point of contact in case of questions or problems.
System Admin Training	The system admin training must cover the below key areas: • Managing the RM&DM&CM platform • Upgrading, installing, and configuring the RM&DM&CM application software and computer hardware • Troubleshooting and providing technical support to employees • Creating and managing system permissions and user accounts • Performing regular security tests and security monitoring • Maintaining networks and network file systems
Business Admin Training	The business admin training covers the training of limited CCT officials who perform records management administrative functions pertaining to: • Building of the classification systems • Updating and amendments to the classifications systems
Power/Super User Training	The power/super user training must enable certain users to perform the below tasks: • Play an essential role in assisting colleagues during instructor-led training sessions and at go-live, ensuring a successful system adoption by end-users. • Provides operational support for the implementation project. • Answer end-user questions, assist the Training Team with end-user training, and serve as a liaison between end-users, project leaders, and department leaders. • The Power/Super User's support assignment will take place during and immediately following go-live.

13.7 REQUIREMENTS FOR MAINTENANCE AND SUPPORT SERVICES ON THE RM&DM&CM SOLUTION

The following provide for the requirements and deliverables for maintenance and support of the RM&DM&CM Solution. Refer to Schedule **D in section (5) Price Schedule**

Deliverable Category	Requirement Description
Maintenance	Ongoing service that ensures the maintenance of the RM&DM&CM solution. This includes: • Fixing faults, • Applying security patches • Enabling new features • Applying any other updates/upgrades that become available for the software that forms part of the RM&DM&CM solution. Maintenance encompasses the end-to-end process from relevant improvements being available for the software, to the testing of these improvements, to the final implementation on the production systems. The service provider would be expected to conform to the City's standard processes in this regard, which include, but are not limited to, the use of distinct test and production environments, as well as governed change control processes.
Support	Support encompasses: • Support requirement is 24 hours a day 7 days a week. • Technical support will be provided by trained CCT staff • All application support will be the responsibility of the appointed vendor

13.8 REQUIREMENTS FOR PROFFESIONAL SERVICES FOR THE RM&DM&CM SOLUTION
The following provide for the requirements and deliverables for professional services for the RM&DM&CM Solution. Refer to Schedule **F in section (5) Price Schedule**

Resource Category	Role Description
RM& DM Technical Consultant	• This is a skilled position that requires extensive experience in a related field along with a high level of education (NQF level of 7 or similar) • Transferring of skills to the relevant CCT officials for continuity • Liaising with clients and stakeholders to determine project requirements. • Determining project parameters, timelines and deliverables. • Building and maintaining an expert knowledge of technology solutions. • Designing and testing a range of software and technical solutions. • Driving the rapid adoption of new technologies, ideas and processes. • Creating user and training documentation and overseeing training sessions. • Using data modelling and analysis to inform and illustrate solutions. • Developing functional specifications for developers to implement. • Creating and testing deployment processes and plans, and overseeing deployments. • Being first point of contact and providing guidance and advice for the duration of a project.
RM& DM Technical Lead	• Provide strong technical leadership and guidance to both CCT and project teams, including teams that are geographically distributed • This is a skilled position that requires extensive experience in a related field along with a high level of education (NQF level of 7 or similar) • Transferring of skills to the relevant CCT officials for continuity • Delegating work and assignments to team members • Collaborating with their team to identify and fix technical problems • Analyzing users' needs and then finding applications to serve them • Creating end goals for their team • Checking that software and applications are updated • Supervising system modifications • Conducting security audits to identify areas of improvement • Guiding their team through technical issues and challenges

Resource Category	Role Description
RM&DM&CM Software Developer	• Researching, designing, implementing, and managing software programs • Testing and evaluating new programs • Identifying areas for modification in existing programs and subsequently developing these modifications • Writing and implementing efficient code • Determining operational practicality • Developing quality assurance procedures • Deploying software tools, processes, and metrics • Maintaining and upgrading existing systems • Working closely with other developers, UX designers, business and systems analysts
RM& DM Project Manager	• Provide strong technical leadership and guidance to both CCT and project teams, including teams that are geographically distributed • This is a skilled position that requires extensive experience in a related field along with a high level of education (NQF level of 7 or similar) • Transferring of skills to the relevant CCT officials for continuity • Plan and Develop the Project Idea • Create and Lead Your Dream Team • Monitor Project Progress and Set Deadlines • Solve Issues That Arise • Manage the budget • Ensure Stakeholder Satisfaction • Evaluate Project Performance

13.10 ABBREVIATIONS

NARSSA	The National Archives and Record Service of South Africa
CCT	City of Cape Town
DoD	The United States Department of Défense
ECM	Electronic Content Management
DM	Document Management
RM&DM&CM	Records Management Document Management and Case Management
RM	Record Management
ISO	International Organization for Standardization
RCM	Public Sector Record Management
SANS	South African National Standards
WCARS	Western Cape Archives and Records Service
CM	Case Managment

13.11   DEFINITIONS

Term	Definition
Document	A document is "recorded information or object which can be treated as a unit." (ISO 12651-2). A document can either be in an analogue or electronic format, for example, and analogue format includes for example paper applications while electronic formats refer to word documents, spreadsheets, PDF's, images and any other, multimedia files, etc.
Record	Records are documents that are "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business". (ISO 15489). There are 4 types of records with different retention periods A record is immutable and cannot be changed.
Documented Information	The ISO 9001:2015 standard no longer uses the RM&DM&CM "documents" and "records". Both are now called "documented information". As per the ISO 9000:2015 definition, the term documented information refers to information that must be controlled and maintained. Therefore, it expects that you also maintain and control the medium as well as the information. The key identifier of a record verses a document is that records are documented information that is "retained" and documents are documented information that is "maintained".
Document Management (DM)	Document Management is the systematic control of documents by predetermined rules, principles and techniques (International Records Management Trust - derived from ISO 9000:2015) Document management is used to track and manage the overall process of document creation, from inception through completion.
Record Management (RM)	The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. (ISO 15489, Part 1, Clause 3.16.)
Document Management System (DMS)	Document Management System (DMS). A system (or application) used for managing documents that allows users to create, store, retrieve, collaborate and share them with security and automated version control. DMSs are sometimes called Electronic Document Management Systems (EDMSs). (DoD 5015.2-STD)
Record Management System (RMS)	An automated system used to manage the creation, use, maintenance and disposal of electronically created records for the purposes of providing evidence of business activities. These systems maintain appropriate contextual information (metadata) and links between records to support their value as evidence.
Records Management and Document Management system (RM&DM&CM)	Refers to computer-based application dealing with the management of documents and records throughout the document and records life cycle (ISO 12651-1:2012) It therefore refers to a system that provides DM and RM functionality where these modules are integrated and supported by workflow with some standard operational procedures. RM&DM&CM are being used in a range of ways to manage digital records and information, including converting a paper file system to a digital system, replacing the use of relatively uncontrolled shared drives, network drives, computer hard drives and personal email folders for the storage of digital information, supporting workflow systems, such as case management as well as providing robust back-end records management functionality.

Term	Definition
Enterprise content management (ECM)	Enterprise Content Management (ECM) incorporates Document, record and case management but also considers additional functionality such as web content management, BPM process maps, BPM simulations, etc. Document and Record Management are at the heart of the ECM.
SAP RCM	It is the union of Records management and Case Management with some additional features focussing, specifically on the public sector. The goal of the RCM is to manage business process-related documents following the public sector laws, rules, and practices. It is a module.
Access	Once the user log into the RM&DM&CM system, the RM&DM&CM system and not the IT controls determine the user's rights, opportunity, means of finding, using or retrieving information, usually subject to rules and conditions as well as regulations and legislation. (Sources: ISO 15489, Part 1, Clause 3.1; International Council on Archives)
Integration	A tightly bound relationship between the different modules of the RM&DM&CM solution and other applications. Integration implies data being shared between systems, a common look and feel that suggests a single application.
Metadata	Refers to data describing the structure, data elements, interrelationships, and other characteristics of electronic records and documents that are securely stored that fulfils the requirements and standards of document and record management (DoD 5015.2-STD). Metadata is data about other data, documents or records that describes their content, context, structure, data format, provenance, and/or rights attached to them (ISO 5127:2017, 3.1.10.26.01). It includes data with regards to Author or Originator, subject or Title, format type, Originating Organization, Date Filed. Publication Date, etc.
Migration	The act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another (SO 15489 – 2002, Part 1, Clause 3.13 and Part 2, Clause 4.3.9.2.).
NARSSA	National Archives and Records Service of South Africa
WCARS	Western Cape Archives and Records Services
Audit trail	Data that allows the reconstruction of a previous activity, or which enables attributes of a change (such as date, time, operator) to be stored so that a sequence of events can be determined in the correct chronological order. Usually in the form of a database or one or more lists of activity data. Sources: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 1. OR An electronic means of auditing the interactions with records within an electronic system so that any activity in the system can be documented as it occurs for identifying unauthorized actions in relation to the records, e.g., modification, deletion, or addition. Source NARSSA.
Extract	A copy of a digital record, from which some material has been removed or permanently masked. An extract is made when the full record cannot be released for access, but part of the record can. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 3. An extract is a copy of a record, from which some material has been removed or permanently masked. An extract is made when the full record cannot be released to a requester, for example under PAIA, but part of the record can. An extract of draft a whole folder is made by creating extracts from some or all of the records which the folder contains. Source NARSSA.

Term	Definition
Enterprise content management (ECM)	Enterprise Content Management (ECM) incorporates Document, record and case management but also considers additional functionality such as web content management, BPM process maps, BPM simulations, etc. Document and Record Management are at the heart of the ECM.
SAP RCM	It is the union of Records management and Case Management with some additional features focussing, specifically on the public sector. The goal of the RCM is to manage business process-related documents following the public sector laws, rules, and practices. It is a module.
Access	Once the user log into the RM&DM&CM system, the RM&DM&CM system and not the IT controls determine the user's rights, opportunity, means of finding, using or retrieving information, usually subject to rules and conditions as well as regulations and legislation. (Sources: ISO 15489, Part 1, Clause 3.1; International Council on Archives)
Integration	A tightly bound relationship between the different modules of the RM&DM&CM solution and other applications. Integration implies data being shared between systems, a common look and feel that suggests a single application.
Integration	A tightly bound relationship between the RM&DM&CM and another application or mechanism. Integration implies data being shared between systems, a common look and feel that suggests a single application. Source: Adapted from New South Wales Department of Public Works and Services, Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B – Specifications, March 2001, p. 13. National Archives of Australia RM&DM&CM Specifications – Glossary 69 & NARSSA.
Retrieve	This term refers to the process of location a specific file, document or record (usually through a search function) and then delivering it as a whole so it can be used by the authorised user by either viewing, editing or print it subject to access rights.
Unique identifier (UID)	A unique identifier (UID) is an identifier that marks that particular record as unique from every other record. It allows the record to be referenced in the Summon Index without confusion or unintentional overwriting from other records.
Turnkey Solution	Turn Key Solution is a type of system built end-to-end for a customer that can be easily implemented into a current business process. It is immediately ready to use upon implementation and is designed to fulfill a certain process such as manufacturing (in part or whole), billing, website design, training, or content management.

(14.1) MONTHLY PROJECT LABOUR REPORT (EXAMPLE)

ANNEX 1

CITY OF CAPE TOWN
MONTHLY PROJECT LABOUR REPORT

CITY OF CAPE TOWN
ISIXEKO SASEKAPA
STAD KAAPSTAD

Instructions for completing and submitting forms

General

1 The Monthly Project Labour Reports must be completed in full, using typed, proper case characters; alternatively, should a computer not be available, handwritten in black ink.

2 Incomplete / incorrect / illegible forms will not be accepted.

3 Any conditions relating to targeted labour stipulated in the Contract (in the case of contracted out services or works) shall apply to the completion and submission of these forms.

4 This document is available in Microsoft Excel format upon request from the City's EPWP office, tel 021 400 9406, email EPWPLR@capetown.gov.za.

Project Details

5 If a field is not applicable insert the letters: NA

6 Only the Project Number supplied by the Corporate EPWP Office must be inserted. The Project Number can be obtained from the Coordinator or Project Manager or from the e-mail address in point 4 above.

7 On completion of the contract or works project the anticipated end date must be updated to reflect the actual end date.

Beneficiary Details and Work Information

8 Care must be taken to ensure that beneficiary details correspond accurately with the beneficiary's ID document.

9 A new beneficiary is one in respect of which a new employment contract is signed in the current month. A certied ID copy must accompany this labour report on submission.

10 Was the beneficiary sourced from the City's job seeker database?

11 The contract end date as stated in the beneficiary's employment contract.

12 Where a beneficiary has not worked in a particular month, the beneficiary's name shall not be reflected on this form at all for the month in question.

13 Training will be recorded separately from normal working days and together shall not exceed the maximum of 23 days per month

14 Workers earning more than the maximum daily rate (currently R450 excluding any benefits) shall not be reflected on this form at all.

Submission of Forms

15 Signed hardcopy forms must be scanned and submitted to the City's project manager in electronic (.pdf) format, together with the completed form in Microsoft Excel format.

16 Scanned copies of all applicable supporting documentation must be submitted along with each monthly project labour report. Copies of employment contracts and ID documents are only required in respect of new beneficiaries.

17 If a computer is not available hardcopy forms and supporting documentation will be accepted.

PROJECT DETAILS

Numbers in cells below e.g (6) refer to the relevant instruction above for completing and submitting forms

CONTRACT OR WORKS PROJECT NAME: (6)		EPWP SUPPLIED PROJECT NUMBER: (6)	
DIRECTORATE:		DEPARTMENT:	
CONTRACTOR OR VENDOR NAME:		CONTRACTOR OR VENDOR E-MAIL ADDRESS:	
CONTRACTOR OR VENDOR CONTACT PERSON:		CONTRACTOR OR VENDOR TEL. NUMBER:	CELL / WORK

PROJECT LABOUR REPORT CURRENT MONTH (mark with "X")

JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	YEAR

ACTUAL START DATE (yyyy/mm/dd)	ANTICIPATED / ACTUAL END DATE (yyyy/mm/dd) (7)

TOTAL PROJECT EXPENDITURE / VALUE OF WORK DONE TO-DATE (INCLUDING ALL COSTS, BUT EXCLUDING VAT)

R

ANNEX 1 (continued)

MONTHLY PROJECT LABOUR REPORT

BENEFICIARY DETAILS AND WORK INFORMATION

CITY OF CAPE TOWN
ISIXEKO SASEKAPA
STAD KAAPSTAD

CONTRACT OR WORKS PROJECT NUMBER:		Year	Month		Sheet	
					1	of

No.	(8) First name	(8) Surname	(8) ID number	(9) New Beneficiary (Y/N)	Gender (M/F)	Disabled (Y/N)	(10) Job seeker database (Y/N)	Contract start date (DDMMYY)	(11) Contract end date (DDMMYY)	(12) No. days worked this month (excl. training)	(13) Training days	(14) Rate of pay per day (R – c)
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
										0	0 R -

Declared by Contractor or Vendor to be true and correct:	Name		Signature	
	Date			

Received by Employer's Agent / Representative:	Name		Signature	
	Date			

(14.2) BBBEE SUB-CONTRACT EXPENDITURE REPORT (PRO FORMA)

TENDER NO. AND DESCRIPTION: ....

SUPPLIER: ....

B-BBEE SUB-CONTRACT EXPENDITURE REPORT

Rand Value of the contract (as defined in Schedule 4: Preference Schedule) (**P***)	R		B-BBEE Status Level of Prime Supplier	

Name of Sub-contractor (list all)	B-BBEE Status Level of supplier[1]	Total value of Sub-contract (excl. VAT)[1]	Value of Sub-contract work to date (excl. VAT)[1]	Value of Sub-contract work to Sub-contractors with a lower B-BBEE Status Level than supplier
Sub-contractor A		R	R	R
Sub-contractor B		R	R	R
Sub-contractor C		R	R	R

[1]Documentary evidence to be provided

	Total:	R
%	Expressed as a percentage of **P***	%

Signatures

Declared by supplier to be true and correct: ....   **Date:** ....

Verified by CCT Project Manager: ....   **Date:** ....

(14.3) PARTNERSHIP/ JOINT VENTURE (JV) / CONSORTIUM/ EXPENDITURE REPORT (PRO FORMA)

TENDER NO. AND DESCRIPTION:

SUPPLIER:

PARTNERSHIP/ JOINT VENTURE (JV)/ CONSORTIUM EXPENDITURE REPORT

| Rand value of the contract (as defined in Schedule 4: Preference Schedule) (**P***) | R | | B-BBEE Status Level of Partnership/ Joint Venture (JV)/ Consortium | |

Name of partners to the Partnership/ JV / Consortium (list all)	B-BBEE Status Level of each partner at contract award	Percentage contribution of each partner as per the Partnership/ JV/ Consortium Agreement[1] **A**	Total value of partner's contribution (excl. VAT)[1] **B = A% x P***	Value of partner's contribution to date (excl. VAT)[1] **C**	Value of partner's contribution as a percentage of the work executed to date **D = C/P*x100**
Partner A		%	R	R	%
Partner B		%	R	R	%
Partner C		%	R	R	%

[1]Documentary evidence to be provided

Signatures

**Declared by supplier
to be true and correct:** _____ **Date:** _____

**Verified by CCT
Project Manager:** _____ **Date:** _____