Part B

Specification for

VERS Compliant Record Keeping System

Tenderers must respond to each clause of this Part by providing a statement of compliance for each clause, or by providing the information requested in the relevant clauses in this Part.

Part B - Specification must be reproduced in full with your responses to each clause and must be provided in
Part D – Tender Form and Vendor Response – Schedule 13.2 – Compliance with Specification.

Where additional information is being provided, a reference must be made to the Schedule in Part D where the information is provided.

April 2000

Contents

1. Goals and Objectives *6*

1.1 Purpose of the Request for Tender **6**

1.1.1 Mandatory requirements 7

1.2 Scope **8**

1.3 Time Frame **12**

Mandatory requirement 12

1.4 Engagement Terms and Conditions **13**

1.4.1 Mandatory Requirements 13

1.5 Implementation **16**

1.5.1 Staff Numbers 16

1.5.2 Volumes 16

1.6 Deliverables **17**

2. VERS @ DOI Implementation *18*

2.1 Overview **18**

2.2 VERS Encapsulated Objects **19**

2.2.1 VERS Format 19

2.2.2 VEO Structure 20

2.3 Folders and Records **21**

2.4 The RKS Record Life Cycle **21**

2.5 Record Creation **23**

2.5.1 Record Capture 23

2.5.2 Encapsulation 24

2.5.3 Registration 24

2.6 Import/Export **25**

2.7 Records Management Functionality **25**

2.8 Discovery **26**

2.9 Reporting **27**

3. Record Creation *28*

3.1 Record Creation Process for VEOs **28**

3.1.1 Overview 28

3.1.2 Record Capture Components 30

3.1.3 Encapsulator 31

3.1.4 Record Capture / Encapsulator API 32

3.1.5 Bulk creation of record VEOs 32

3.1.6 RKS creation of records 33

3.1.7 Requirements for Record Creation of VEOs 33

3.2 Record Creation Process for Paper Records **44**

3.2.1 Requirements 44

4. Import/Export of Records/Folders *45*

4.1 Export of Records **45**

4.1.1 Requirements for Export of Records 46

4.2 VEO Import **48**

4.2.1 Requirements for VEO Import 48

5. RKS Records Management Functions *51*
5.1 General Records Management **52**
5.1.1 Classification Structure 52
5.1.2 Thesaurus 53
5.1.3 Controlled Vocabularies 54
5.1.4 Folder Maintenance 54
5.1.5 Record Maintenance 57
5.1.6 Record Types 58
5.1.7 Disposal of Records 59
5.1.8 Workflow for records management 62
5.1.9 Records Manager In-Tray 63
5.2 Paper Records Management **64**
5.2.1 General Functions 64
5.2.2 Barcode Functions 65
5.2.3 Tracking Functions 65
5.2.4 Archival Functions 66
6. Discovery *67*
6.1 Overview **67**
6.2 Web Access **69**
6.2.1 Search Record Keeping System 69
6.2.2 Display Object 70
6.2.3 Recover Documents 71
6.3 Requirements for Discovery **72**
6.3.1 Discovery Web Interface 72
6.3.2 Discovery and delivery API 78
7. Reporting *79*
7.1 Reporting Tools **79**
7.1.1 Requirements 79
8. Authentication (Digital Signatures) *84*
8.1 Authentication and Audit **84**
8.1.1 Digital signatures 84
8.2 Public/Private Keypair Management **86**
8.2.1. Certificate Records 86
8.2.2 Signature Management 87
9. Security & Audit *88*
9.1 Security – Records & Users **88**
9.1.1 Access Control Policy Management 89
9.1.2 Control of access to folders and records 90
9.1.3 Control of access to system functions and facilities 92
9.2 Audit **94**
9.2.1 Requirements 95
10. System Management Functions *97*
11. Implementation, Training, Documentation and Support Considerations *104*
11.1 Phased Approach **104**
11.2 Training Approach **104**
11.3 Training Courses **104**
11.4 Documentation **105**
11.4.1 Types of Documentation 105

11.4.2 Format of Documentation 106
11.4.3 Customisation and reproduction of documentation 106
11.5 System Support 106
11.6 Operational Support 107
11.7 Service Level Issues 107
11.7.1. On-going Development 107
11.7.2 Customer Service Framework 107
11.7.3 Performance Standards 108
12. Technical Requirements & Design Considerations 109
12.1 Ease of use 109
12.1.1 Mandatory requirements 110
12.2 Capacity 110
12.2.1 Estimated Capacity Requirements 110
12.2.2 Capacity Issues 111
12.2.3 Mandatory requirements 111
12.3 Availability 112
12.3.1 Mandatory requirements 112
12.4 Reliability 112
12.4.1 Mandatory requirements 112
12.5 Maintainability 113
12.5.1 Mandatory requirements 113
12.6 Web enablement 113
12.7 DOI Technical Environment 114
12.7.1 Mandatory Requirements 114
12.8 Development Environment 115
12.8.1 Mandatory Requirements 115
12.9. Data Migration 116
12.9.1 Mandatory Requirements 117

1. Goals and Objectives

1.1 Purpose of the Request for Tender

The VERS @ DOI project will implement the Victorian Electronic Records Strategy (VERS) within the Victorian Department of Infrastructure (DOI). A brief description of the background to this project can be found in section 1.4.

This tender is based on the framework already established in previous projects conducted by Public Record Office Victoria (PROV), CSIRO and Ernst & Young. Tenderers should familiarise themselves with the *Victorian Electronic Records Strategy Final Report* and the Public Record Office Standard PROS 99/007 – *Management of Electronic Records.* These documents, as well as other related information, are available on the PROV web site http://www.prov.vic.gov.au/vers/ .

The VERS @ DOI project has two major goals:

- To implement a functioning electronic Record Keeping System (RKS) which will enable the capture, retention and management of DOI business records in a central corporate electronic repository which has the responsibility for long term preservation.
- To act as a demonstrator system for VERS for potential use by other Government Agencies (at the local, state, and federal level), and Public Record Office Victoria.

A record keeping system (RKS) is needed to assist DOI in applying records management practices to both paper and electronic records and support the medium to long term information needs of the business. It is also essential in building and maintaining the corporate memory and providing the central repository to support effective knowledge management and e-business initiatives. The RKS should

- manage a corporate classification and filing structure,
- ensure the integrity and reliability of records once they have been captured,
- specify explicit disposal schedules (which determine how long records should be kept and how they should eventually be disposed – either destruction once the records are no longer needed, export to another government agency, or export to PROV for permanent preservation.), and
- maintain information about responsibilities as described in AS 4390.2 1996.

Electronic document management (EDM) is different to electronic record keeping in that EDM systems support the short-term operational requirements for accurate creation and control of business documents (i.e. work in progress).

The record keeping system should be capable of managing paper and electronic records throughout their lifecycle, from capture and registration through 'trusted record-keeping' to eventual destruction or permanent preservation, while retaining integrity, authenticity and accessibility. This document sets out the requirements for a record keeping system that is compliant with the Victorian Electronic Records Strategy.

The broad objectives to be achieved as a result of this project are:

- To store and manage electronic records in accordance with the Victorian Electronic Records Strategy and PROS 99/007 – *Management of Electronic Records* so that they may be located and viewed (as they were originally created) over an extended time frame.
- To provide a method for ensuring the authenticity of the records captured, that is, that the records have not been altered or tampered with. This will be achieved by the use of digital signatures.
- To accept electronic records from a variety of sources including electronic mail, computer files from the disk system, desktop applications, Electronic Document Management systems (EDMS), Lotus Notes applications, scanned images, etc.
- To migrate records from existing Records Management Systems.
- To enable the recording and tracking of paper based records alongside electronic records.
- To implement security and access control to ensure appropriate probity and privacy principles are applied to the records.
- To provide web based searching, browsing and retrieval mechanisms to allow authorised users to find and view the records. (Global search tools across the DOI electronic data repositories should include the RKS.)
- To provide management functions that allow the department to centrally manage the records contained within the RKS.
- To implement a system to assist the Department in the implementation of consistent corporate record keeping practices including disposal schedules.
- To enable the export of records among VERS compliant record keeping systems in other Government Agencies and PROV.
- To develop a system which is scalable for whole of Victorian Government (WOVG) use.

1.1.1 Mandatory requirements

B1.1 The RKS must comply with the most recent Standard issued by PROV, PROS 99/007 – *Management of Electronic Records*, which advises Government Agencies on the way they should manage electronic records and the format that VERS encapsulated records must be exported to PROV. This Standard is essential reading and should be read in conjunction with this tender.

B1.2 The RKS must comply with recommendations on the most appropriate media usage for VERS. These recommendations are incorporated in PROS 99/007 – *Management of Electronic Records*: Specification 3.

1.2 Scope

The Record Keeping System will initially support the business of the Department of Infrastructure but the requirements for management of corporate long-term records are common across all Government agencies. The Record Keeping System proposed must be scalable for any sized organisation.

The Department of Infrastructure is responsible for the coordination of a number of separate Agencies. The Department provides corporate services, such as Records Management, to some Agencies and these Agencies are included within the scope of this tender and implementation. Where the tender refers to DOI it also includes these Agencies that DOI provides with a Records Management service. The Agencies will have separate disposal schedules, access control policies, and classification structures to manage their records.

This tender is for the implementation of an in-house system based at DOI only, and will need to support the Agencies serviced by DOI.

The initial implementation will be a pilot functional model for DOI. If the DOI project is successful and the project is scaled to the whole of Victorian Government (WOVG), then a subsequent tender will be initiated to consider portal and out-sourcing models at that stage. The WOVG model may be a separate electronic repositories for each agency, or one massive database for WOVG with centralised management. It is expected that the successful tenderer would be involved in presentations and demonstrations of the pilot DOI model to WOVG.

The VERS @ DOI project will implement a functional record keeping system that captures and manages records in the VERS Encapsulated Object format. More details about VERS encapsulated objects may be found in section 1.5.

The successful tenderer will be required to perform the following tasks:

- Supply, install, and commission a Record Keeping System with the characteristics described in this tender specification
- Provide training of nominated DOI and Agency staff in aspects of the system
- Provide on-going support for the system.

This tender makes as few assumptions as possible about the technical means by which the RKS functionality will be delivered. It is expected that Tenderers will have significant experience in the design and implementation of electronic record keeping systems and will have a sound knowledge of the best means of constructing the appropriate system.

The system supplied must be functional and user friendly. This means that it must be intuitive, integrate smoothly with other common desktop applications, process commonly used functions within a reasonable response time, be reliable, have minimal down time, and offer the range of functionality required.

In most situations, users will need to initiate the process to create records. Users should be unaware of any complex technical processes (e.g. conversion to XML and

the application of digital signatures) that happen behind the scenes to encapsulate electronic objects and manage records in the RKS.

The records to be captured in the RKS will come from a variety of sources including word processing, spreadsheets, electronic mail, web pages, Lotus Notes databases, scanned images, fax server, etc. The RKS must be able to encapsulate all electronic objects, though different preservation formats may be used according to the object type. The types of objects to be encapsulated as VEOs and registered in the RKS will be progressively introduced over the phases of the project, with the most common and simple electronic objects being tackled first.

Records stored in the RKS will be kept for the period set by a disposal schedule. Depending on the type and source of the record, this may be for an extended time frame, possibly up to 100 years or more. The RKS proposed must be capable of storing and managing electronic objects for extended time periods. Media refresh strategies will need to be defined.

Agencies with VERS compliant record keeping systems may have the need to export records to other VERS compliant record keeping systems. The RKS must provide an Import/Export capability to enable this export of records. Records will routinely be exported in batches to PROV according to the nature of the records (i.e. permanent value only) and according to the disposal schedule applicable to the records.

The records in the RKS must not be lost or destroyed irrespective of what event occurs, including power failures, corruption of internal databases, storage media failure, copy failures, etc. The export processes between systems must ensure that suitable verification checks are in place to verify that no records are lost during the export.

Tenderers will be expected to provide a total solution. The solution may encompass a variety of products from different suppliers. It will be the party responding to this tender who will have overall responsibility to integrate the product set proposed and manage the supplier relationships.

The products and services to be provided in response to this RFT are:

- Project Management services to assist with finalising the system details and project plan prior to commencement of work
- The supply of any package software complete with enhancements required
- The development of integration and other software required to supply the total solution
- Advice on (but not the supply of) the recommended hardware configuration
- Recommendations on the most appropriate data storage mechanisms and media (considering both the initial implementation and potential scalability)
- Technical services to implement the solution
- Assistance with the set up of system management functions such as back-up strategy, DBMS toolkit, migration tools, etc.
- On-site support and training during the pilot stage

- On-going support of the system, including software upgrades
- Training services in the development of appropriate training options for staff
- Provision of training services as agreed
- Supply of detailed system documentation
- Project management of any consortium group involved in the provision of the products and services
- Migration strategy and utilities to migrate records from existing Records Management Systems
- Advice on the system scalability to WOVG.

The scope of the VERS RKS functionality is:

- To interface to a variety of document capture and workflow systems
- To enable the capture of a vast range of electronic objects in the required long term format
- To encapsulate electronic objects into the VERS Encapsulated Object format
- To register the encapsulated objects into the RKS
- To provide records management functionality to manage the records in the RKS
- To include functionality to manage paper based records alongside electronic records
- To provide adequate controls to ensure the security of the data contained in the RKS, e.g. access control
- To provide a web based discovery capability to locate and view the records using different search strategies
- To enable documents within a record to be viewed as they were originally created
- To recover documents back in their original format from a record to allow the reuse of the content. The record itself cannot be modified.
- To enable the authentication of electronic records by the use of digital signatures
- To develop mechanisms to enable the export of records among VERS compliant record keeping systems
- To provide as much web based RKS functionality as possible
- To establish media migration strategies to ensure physical preservation of the electronic records
- To ensure that the system proposed is scalable to WOVG proportions.

The knowledge gained in the early phases of the implementation will assist in confirming the details of the requirements for later stages.

The VERS encapsulated objects (VEOs) must be portable to future systems and/or media without any loss of information. That is, the original document content and metadata must be retained as an exportable object to future systems without dependency on data held in the originating VERS compliant record keeping system.

The RKS may potentially incorporate as part of the total solution:

- specialist electronic records management products which have demonstrated an ability to integrate with supporting technologies, as well as fully integrated 'all-in-one' product solutions
- products aimed at the large multi-site departments with tens of thousands of users, as well as those aimed at small, single-site organisations with a few hundred users
- products developed for an Intranet environment, as well as those developed for use across an enterprise local area network.

The primary focus of this tender is the supply of a record keeping system but ancillary functions that would be desirable are:

- A facility for electronic document management of active documents, i.e. Check-in/check-out, version control, etc.
- Integration with a workflow facility
- Integration with image scanning systems.

1.3 Time Frame

The VERS @ DOI project has been granted funding to have a functional system in place and operational in DOI by June 2001. The success, or otherwise, of the project will be assessed at that stage to determine if further funding is justified to extend the project to whole of Victorian Government (WOVG). Another tender would potentially be issued at that stage to investigate out-sourcing options.

To achieve the deadline, the technical and design specification for a basic functioning VERS compliant record keeping system should be agreed to by the last quarter of 2000. It is intended that the project be phased so that functionality is progressively introduced over a period of time to an increasing user base, rather than implemented in one hit to all staff. The initial system, implemented by June 2001, will cover the basic requirements to capture, manage and discover electronic records. A pilot group will be selected for the initial implementation. System functionality and the user group will be widened during the phases in the third and fourth quarters in 2001. Aspects of paper record management, including the migration from existing systems, will be addressed after the initial implementation subject to funding and the success of the initial system. However the provision of this functionality for paper records does form part of this tender.

The phases of the VERS @ DOI implementation are subject to alteration in consultation with the successful tenderer on the best approach, but they are envisaged to be:

Phase	Imp. Date	Implementation Phase	Functionality
1	Qtr 4 2000	Design	Detailed technical and design specification
2	Qtr 2 2001	Pilot System	-Capture documents from the file system -Capture Lotus Notes electronic mail -Encapsulate electronic objects into the VERS format -Register records and folders into the RKS -Discovery -Implement access control -Records management functionality -System management functionality -Implementation in 2 business units
3	Qtr 3 2001	DOI Production System	-Import/Export of VERS Encapsulated objects -EDMS record capture interface -Capture of other types of Lotus Notes documents -Paper records management -Full system functionality -
4	Qtr 4 2001		-Implementation in DOI -Extended range of document capture interfaces
5	Qtr 1 2002		-Migration from existing Records Management Systems

Mandatory requirement

B1.3 A detailed project plan will be required as part of the tender response in Part D Schedule 4.

1.4 Engagement Terms and Conditions

1.4.1 Mandatory Requirements

1.4.1.1 Probity

B1.4 An essential prerequisite for selection of the Supplier in response to this Request for Tender is a declaration by the Tenderer. The tenderer should advise the Department of any matter or issue which is, or may lead to, a conflict of interest regarding current or proposed services to the Department of Infrastructure and/or its agencies, or other Victorian Government departments or funded agencies. The Tenderer should also state how any such potential conflict of interest may be avoided.

1.4.1.2 Reporting Structure

B1.5 For the duration of the assignment the Contractor will report to the VERS Project Director.

B1.6 The successful Tenderer will be required to submit a detailed project plan indicating key milestones in the implementation of the proposed solution.

B1.7 On a fortnightly basis, the Tenderer will be required to report to the Project Director on the progress of the project and where, if any, milestones are late or have not been achieved.

1.4.1.3 Confidentially and Disclosure of Information

B1.8 The Contractor shall not, without prior written approval of the Department (which approval shall not unreasonably be withheld) make public or disclose to any person any information about the Department's confidential information, this Agreement, or any other matter associated with this Agreement, and in giving written approval the Department may impose such terms and conditions as it thinks fit.

B1.9 The Contractor shall take all reasonable steps to ensure that its employees or agents do not make public or disclose information referred to above.

B1.10 The Department may at any time require the Contractor to execute, and arrange for its employees or agents engaged in the performance of this Agreement, to execute a Deed of Confidentiality relating to the non-disclosure of the Department's confidential information and the Contractor shall arrange for all such Deeds to be executed promptly.

B1.11 Subject to this Agreement expressly allowing the Department to disclose certain information, the Department shall:

- ♦ treat as confidential all information obtained form the Contractor which is clearly marked as being confidential or obtained in circumstances inferring confidentiality: and

- not disclose to any person without the consent of the Contractor (which consent shall not reasonably or unlawfully withheld) any information referred to in the sub-clause above.

B1.12 The obligation of the Contractor and the Department under the above sub-clauses shall not be taken to have been breached where the information referred to in those sub-clauses:

- is or becomes public knowledge other than by breach of the above sub-clauses
- is in possession of the receiving party without restriction in relation to disclosure before the date of receipt from the disclosing party:
- is legally required to be disclosed; or
- has been independently developed or acquired by the receiving party.

B1.13 Nothing in this clause shall be construed to prevent the Department from disclosing any information provided by the Contractor to any other Victorian Government Department or Agency provided that, if the information is confidential information, the Department takes all reasonable steps to ensure that such information is treated as confidential by such Departments and Agencies and their servants or agents, including, where appropriate, requiring those people to enter into suitable confidentiality agreements.

1.4.1.4 Termination of Assignment

B1.14 The Department reserves the right, on written notice, to terminate, reduce or amend any assignment commenced by the Contractor. Payment of costs will be made for satisfactory work completed at that time.

1.4.1.5 Non-Soliciting of Staff

B1.15 Except with the prior written consent of the other party to the Agreement, neither party shall solicit for employment, engagement or hire, any officer or member of staff of the other party for a period of two years from the date of commencement of this Agreement.

1.4.1.6 Project Steering Committee

The development and implementation will be managed by a Project Steering Committee, as per GITC, whose members have been drawn from:

- DOI Executive Director (sponsor)
- Senior DOI Executives
- Public Record Office Victoria
- Multimedia Victoria

The Steering Committee meetings are attended by the VERS Project Director.

The Prime Contractor's Project Manager and one other senior representative will also be invited to attend Project Steering Committee meetings.

1.4.1.7 Contractor's Staff

B1.16 Tenderers shall name staff for both the project management and other tasks in the contract.

B1.17 Tenderers may during the course of the contract, replace staff with someone acceptable to DOI who has equivalent or greater knowledge and experience subject to DOI written agreement. DOI reserves the right to veto any replacement staff.

B1.18 Tenderers to provide a Curriculum Vitae for each member of staff proposed for the contract.

1.4.1.8 Payment Schedule

B1.19 Progress payments, if proposed, shall be linked to specific deliverables.

1.4.1.9 Intellectual Property

B1.20 All intellectual property rights in the developed software or other items that are specifically developed for DOI under this Contract are assigned to the State of Victoria. Ownership of pre existing intellectual property rights in any tools, object libraries and methodologies used to produce the developed software or other items, will not be affected. GITC contract provides three options for Intellectual Property in clause 21, and the first option (as stated above) will be the one used for this contract. The other options will be deleted from the contract.

1.4.1.10 GST

B1.21 The Tenderer must provide its Australian Business Number (ABN). Tenderers are advised that if no ABN is supplied, then PAYG Withholding Tax may apply and the Department is required by law to deduct the relevant amount from any payment under the Contract and to remit the relevant amount to the Australian Taxation Office.

B1.22 Any invoice submitted must be in the form of a Tax Invoice consistent with GST Law.

1.5 Implementation

It is envisaged that the RKS will be implemented in two phases:

- Pilot implementation in two business units
- Complete implementation across the Department (including all regional locations) and Agencies to which the Department provides a Records Management Service.

1.5.1 Staff Numbers

The Department currently employs approximately 750 staff. All staff members currently have read access to the existing Records Management System. Approximately 30% of staff have update access to the records Management System, and 10 staff members have access to the System Management functions. It is expected that this pattern of access will change in the new Record Keeping System as all staff will require the ability to add records to the RKS.

These staff members are located at the following locations:

- Nauru House, Melbourne CBD – majority of staff
- North Melbourne - 48
- Sunshine - 14
- Burwood - 16
- Ballarat - 10
- Benalla - 6
- Bendigo - 5
- Geelong - 8
- Traralgon -8

1.5.2 Volumes

The following figures are estimates:

- Network File System disk space usage is 250GByte with a growth of 10 GByte per month
- Electronic Mail - up to 800 MByte per day sent & received, or 16 GByte per month. Approximately 40 GByte of electronic mail is stored at any time.

The existing Records Management System currently manages about 200,000 folders and 300,000 records (most records are not registered, but are on folders).

1.6 Deliverables

Tenderers are requested to provide details of how you intend to provide the deliverables in Part D Schedule 4. It is expected that the deliverables will include:

- Project Plan
- Detailed technical and design specification
- Initial system to capture, manage, discover and store electronic records
- Record Capture System for File System
- Record Capture System for Notes email and bulk capture of email
- Discovery system, reporting system
- Import/Export of VEOs and File VEOs
- Record Capture System for EDMS
- Record Capture System for other Notes documents including teamroom and outgoing faxes
- Record Capture Interface for web pages
- Paper file management
- Record Capture System for desktop applications, Microsoft Office and Visio, fax interface
- Record Capture interface to scanners
- Migration tools for existing Records Management Systems (Recfind, Trim)
- Disaster Recovery/Business Continuity Plan
- Service level agreement and 5 year support plan
- Change management and release/upgrade procedures
- Project management – project reports, revised plans, issue register
- Implementation – strategy, plan, schedule
- Training – training plan, course content, training schedule
- Documentation - RKS related, and technical
- Recommended RKS Environment - hardware, software, database, backup, media management, system monitoring, cipher suites.

2. VERS @ DOI Implementation

2.1 Overview

VERS@DOI is concerned about the management of electronic and paper records at all stages in their life cycle and the integration of all of the systems used to manage them.

The VERS Record Keeping System (RKS) will vary from conventional Records Management Systems (RMS) in that, as well as providing RMS functionality, it will also capture and manage electronic objects as VERS encapsulated objects. This means that the RKS will:

- Be able to convert electronic objects into VEOs
- Enable the registration and management of VEOs and paper records
- Have provision to import VEOs from other Agencies
- Be able to formulate records as VEOs for export to VERS systems at other Agencies and PROV
- Index and display all VEO content and metadata through a discovery facility
- Index and display record metadata held in the RKS management system (i.e. Metadata held externally to the VEOs).

Paper records are currently managed by independent systems, e.g. RecFind. However, a single corporate view of the records regardless of their format is required by DOI. The discovery module will reference both paper and electronic records.

The components that make up the RKS can be identified as:

- Record Creation (incorporating capture, encapsulation and registration)
- Records Management
- Discovery
- Reporting
- Authentication
- Security and Audit
- Import/Export
- System Management

An illustration of this can be found in **Part A – Annexure G – Figure 3: VERS @ DOI Model.**

A functional diagram can also available in **Part A – Annexure G – Figure 4 : VERS @ DOI Functions.**

2.2 VERS Encapsulated Objects

2.2.1 VERS Format

A VERS format record can be thought of as the original data file (the 'Content') wrapped within metadata that describes what the data file is and how it is formatted. Any content format can be contained within a VERS record (e.g. PDF, Word, an Excel spreadsheet, a WAV file, a program), but some of these formats are better for long term preservation than others.

The metadata chosen as most appropriate for VERS is a superset of the National Archives of Australia (NAA) *Recordkeeping Metadata Standard for Commonwealth Agencies*. This means that any metadata that can be expressed in NAA, Australian Government Locator System (AGLS), or Dublin Core can be expressed in VERS. Other descriptive metadata elements can be added to the objects without affecting the fundamental VERS structure. VERS can consequently be easily extended to contain the Australian and New Zealand Land Information Council (ANZLIC) elements that are not currently included in the VERS metadata set.

VERS addresses the issue of preservation of related records by linking the components of a business record together into a 'time capsule' with the contents preserved in a relatively long term format, e.g. PDF, and the contextual information about the record (metadata) wrapped around the contents. Changes to the record are then recorded in the 'time capsule' by adding a fresh layer of metadata (this is referred to as an 'onion' record). The metadata information is stored as XML.

This 'time capsule' contains the history about the life of the VERS encapsulated object (VEO) and remains intact wherever the VEO is exported to regardless of the system used to manage the records.

The contents of a VEO can be signed using digital signatures. These allow a future user to prove when the record was created, that the record has not been subsequently modified and provide some evidence as to who created the record.

The VERS @ DOI system will store documents in two encodings – the original format and the long term encoding, e.g. PDF being the long term format in the case of document type records.

2.2.2 VEO Structure

VERS uses an encapsulation approach to preserve electronic records. The content of the record is wrapped (encapsulated) in an envelope that describes what the content is, how the content relates to other records, and how to interpret the content. The encapsulated object is referred to as a VERS Encapsulated Object (VEO).

A Record VEO can contain multiple documents, and each document can be represented by multiple encodings (refer to the diagram in **Part A – Annexure G – Figure 1: VEO Format and Example**). In its widest sense a document may be a sound file, an image, a digital video or any other recorded information format as well as the more traditional word processing document or electronic mail. All documents within a VEO are related and together form the record.

For example, this RFT forms a record. The RFT consists of four documents (Part A, Part B, Part C, and Part D). Each of these documents is a separate computer file, but must be read in conjunction with the other three parts. The parts of the RFT may be stored in many different formats: Word files, PDF files, HTML files, etc. An encoding is simply one of these formats. A VEO must contain at least one encoding of each document, but may contain multiple encodings (e.g. a PDF and Word version of each document). A diagram of this can be found in **Part A – Annexure G – Figure 1: VEO Format and Example.**

A VEO can store data in any format, however, some formats are more suitable for long term preservation than others. The most suitable formats are those whose structure is documented by a published standard. A published standard allows a viewer or access application for the format to be re-written in the future, if this proves necessary. For the purposes of this tender, the approved long term format for documents is PDF, although other long term formats may be approved during implementation to handle different types of electronic objects.

There are two types of VEOs:

- File VEOs and
- Record VEOs.

A File VEO is created from an RKS folder when the Record VEOs are being exported. The folder within the RKS is a collection of related records grouped to enable easier management of the records.

Further details on the structure of VEOs may be found in PROV *PROS 99/007* Standard for the Management of Electronic Records specification. The *PROS* also provides details of the generic VERS record structure specification, details the VERS metadata scheme specification, and defines the record format specification.

All diagrams referred to in the tender documentation can be found in **Part A – Annexure G**.

2.3 Folders and Records

A fundamental requirement of the RKS is the organisation of records into cognate groups for access, management and eventual disposal. The use of folders, to which records are allocated, facilitates this. Folders provide a means of managing related records as a single unit, for purposes of scheduling, review, preservation and destruction, so that a management process is reliably applied to all records in the group at the same time.

Folders are equivalent to conventional paper files but the word 'folder' has been used to prevent confusion with files in a computer.

The use of folders ensures the comprehensive and reliable retrieval of a complete group of records that relate to the same business activity, case or theme, so that the context of an individual record and the narrative of a sequence of records are preserved.

Management functions may be applied to individual folders, or groups of folders, and hence all associated records.

The RKS will use folders as the primary focus for managing records. As records are registered into the RKS, they must be allocated to folders. The records will then assume the security and classification characteristics of the folders to which they are attached.

2.4 The RKS Record Life Cycle

The RKS will accept electronic objects and convert them to VEOs via the capture and encapsulation process. Once they are in the RKS they are considered to be records. The RKS will manage different types of records:

- Electronic records as VEOs and
- paper based records.

All electronic objects that form a record will be encapsulated and stored as a VEO in the RKS.

In the case of paper records, the RKS will manage the metadata only, it is not intended to scan all paper documents. The metadata may be held in VEO format, but this is not mandatory. However it will be necessary to convert the metadata related to a paper record to VEO format when it is exported from the RKS.

Folders will be created within the RKS and will hold both electronic and paper records. Folders will need to be turned into File VEOs when they are exported from the RKS to another Agency or PROV.

Some information about folders and records will be best held and managed externally to the records. Characteristics such as classification and security, which vary over time and according to changing management requirements, may be held as metadata managed by the RKS.

It should be noted that the content of a VEO (documents and metadata) cannot be changed once in the RKS, because it has been digitally signed. If it is necessary to amend or augment the VEO metadata, then an onion VEO will be created, either immediately the change occurs or when the record is exported. In an onion VEO, the altered metadata is wrapped around the original VEO and another digital signature applied. It is not expected that the RKS will generate a new layer of metadata for each change made to the VEO, instead the changes will be tracked in the RKS audit trail until the record is required to be exported, or an onion layer is applied within the RKS.

When it is necessary to export records to another system, the VEOs will be formed using the original VEOs as the base and a new layer of metadata will be wrapped over the top taken from the management and use history maintained by the RKS. It may not be necessary to export details of all events in the record's history to the receiving Agency, so only the current details may be layered on to the VEO. An example of this would be if records are re-classified a number of times then the interim classifications would not be exported, only the initial and final classification.

All folders and records exported from the RKS will be in VEO format. Folders and paper records will be converted to VEOs and file VEOs incorporating the relevant metadata from the RKS.

The life cycle of records and folders in the RKS is illustrated in **Part A – Annexure G – Figure 2: RKS Record Life Cycle**

2.5 Record Creation

The VERS @ DOI model has three conceptual processes in the creation of RKS records:

- Record capture
- Encapsulation
- Registration into the RKS

Records may also be received by the RKS from other VERS systems, but these will already be in VEO format. Import and export of records will be covered in a later section.

2.5.1 Record Capture

The VERS concept is that any type of electronic record may be stored in the RKS. The implementation of VERS at DOI will be phased so that initially only documents (i.e. those objects that can be printed) will be captured. These objects have been targeted primarily because they represent the majority of documents used to conduct DOI business. The document types included will be:

- Electronic documents such as Microsoft Word documents, Excel spreadsheets and charts, PowerPoint presentations, MS Project charts, VISIO diagrams, etc.
- Electronic mail (from Lotus Notes mail)
- Documents managed by the Electronic Document Management System
- Other documents generated by Lotus Notes, such as teamroom documents, outgoing faxes and web pages
- Metadata from the Records Management system
- Scanned images.

In later phases, the capture of other objects will be considered. These will require different capture processes for each data source and may include:

- Records from Lotus Notes databases, Access databases, etc.
- Database reports such as from Oracle Financials, Fleet Management, etc.
- Archived data from Legacy systems as they are closed down.

Documents may be captured from the application that created them, e.g. Word, or directly from the network disk system (referred to as the file system). Records may be captured individually or in bulk.

2.5.2 Encapsulation

Encapsulation is the process of creating a VEO from the original content and metadata. There may be multiple documents that form the content of the record. Each original document will be incorporated into the VEO in two formats called encodings. One encoding will be in the format used to create the document, and other encoding will be in the VERS long-term format (PDF).

The metadata will be stored in XML as a wrapper around each document and will relate to both the source format encoding and the PDF encoding. The VEO metadata will include details provided by the capture system such as the document date, author, subject, etc.

The encapsulated object will form a VEO.

The encapsulation process will apply digital signatures to the VEO to allow the detection of modifications.

2.5.3 Registration

The VEOs will be registered as records in the RKS. Each record will be allocated to a folder and will inherit the classification and security profiles from that folder. Before being accepted into the RKS the completeness of the information provided in the VEO will be checked. If a user has initiated the capture of the record, then the user will allocate the record to a folder. If the record capture is an automated process, then the rules governing the allocation of the record to a folder will need to be defined as part of the automated process. In some cases the automated process may trigger the creation of a new folder before allocating the record.

An unique identifier will be allocated to each record registered into the RKS. This identifier must be fed back to the originating system so that it may be stored against the original document as a record of its export to the RKS.

2.6 Import/Export

Records of permanent value may be exported to PROV according to the disposal schedule applied to them. Records may be exported to other Agencies as the functions of Agencies may be exported or amended after elections or departmental re-structures.

The records exported will be in VEO format with a fresh layer of metadata applied to indicate current management and use details and the fact that they have been exported. Agency details, date of export, etc. will be included in the metadata.

Likewise, records may be imported from other Agencies and passed through the registration process. Records passed between Agencies and PROV will only be in VEO format.

2.7 Records Management Functionality

The records in the RKS will require management in a similar manner as that provided by a traditional RMS. The range of functionality that will be required includes:

- Classification Structure
- Thesaurus
- Controlled Vocabularies
- Folder Maintenance
- Record Maintenance
- Record Types
- Disposal of Records
- Workflow for records management
- Record Manager In-Tray
- Paper records management (incl. Barcode, Tracking & Archival functions).

2.8 Discovery

The Discovery Module will be the primary user interface that supports users finding and retrieving records from the VERS Record Keeping System. This module will enable users to search records in a variety of ways:

- Search on free text / keywords (including seamless search across paper and electronic records)
- Browse structured views using the RKS classification structure
- Browse related (linked) records.

The Discovery Module will be web based and will display both the record and folder information. Both metadata and content will be available. The history of the records (i.e. versions, re-classification, amalgamations, etc.) and metadata detail may be displayed. Other details of interest such as the number of times the record has been accessed, the last date of access, etc. may be provided, but this is more of an administrative function.

Access to a record is defined as the display of the record metadata and/or contents of the record. Details of access to a record will need to be recorded in the audit log and the management history of the record. The listing of a record in a search result or report is not considered to be an access of the record.

Although it is envisaged that the users wanting records will usually search on-line, it is possible that in future, batch requests for searches may be required.

The Discovery Module must provide a view of the RKS classification structure to allow users to browse the records by classification. This will assist users in narrowing down the search for the information.

The Discovery Module must understand the structure of the VEOs and metadata to display the information in a meaningful way for the users. It must also understand relationships between VEOs. For example, the identification of all records related to a folder. The Discovery Module must also understand (and display if required) the metadata held in the RKS that is not in VEO format. Examples are audit log details, paper record information, etc.

Access to the Discovery Module will be controlled by identification of the users accessing it. Users will be registered with the level of access that they are allowed, that is, which groups of records they are allowed to see and view. Cases where users do not have the access rights to the data they are seeking may have to be handled by the Records Manager.

The search tool will also need to recognise the security applied to the records and match it with the user profile before allowing access to the records.

In the future, searching may be done across whole of Victorian Government VERS repositories. DOI would favour a search tool that enables a global search strategy across other existing DOI databases as well as the VERS RKS repository.

2.9 Reporting

Those using the RKS will require a variety of reporting tools for the production of statistical and descriptive reports. The types of reports will be similar to those produced by traditional RMS. There is a need for standard reports that can be triggered easily as well as the ability to define ad hoc reports.

3. Record Creation

The process of Record Creation involves capturing records and registering them within the Record Keeping System. The RKS will manage two categories of records

- Records that consist of electronic documents that are encapsulated (VEOs)
- Paper records.

In most situations, users will need to initiate the process to create records. Users should be unaware of any complex technical processes (e.g. conversion to XML and the application of digital signatures) that happen behind the scenes to encapsulate electronic objects and manage records in the RKS.

The records to be captured in the RKS will come from a variety of sources including word processing, spreadsheets, electronic mail, web pages, Lotus Notes databases, scanned images, fax server, etc. The RKS must be able to encapsulate all electronic objects, though different preservation formats may be used according to the object type. The types of objects to be encapsulated as VEOs and registered in the RKS will be progressively introduced over the phases of the project, with the most common and simple electronic objects being tackled first.

3.1 Record Creation Process for VEOs

3.1.1 Overview

The process of Record Creation involves capturing records from originating systems and registering them within the Record Keeping System. As part of this process, the records are converted to VERS Encapsulated Objects (VEOs). An originating system may be any software within DOI, including desktop applications such as Word and Lotus Notes; corporate applications such as HR and Financial Systems; and system software such as the file system.

Specific originating systems have been identified for the purposes of this tender. It is expected that the number of originating systems integrated with the RKS will increase over time.

The creation of records may be considered as a single process divided into two parts. The part of the process that is specific to a particular originating system is contained within a Record Capture Component, and the part that is common to all originating applications is contained within the Encapsulator.

A conceptual diagram of the Record Creation Process can be found in **Part A – Annexure G – Figure 5 Record Creation Process.**

A Record Capture Component is tightly coupled to a particular originating system, and will normally be written specifically for that system. This tender will require Record Capture Components to be written for a small number of important originating systems. These include:

- File System (mandatory)
- Lotus Notes (mandatory)
- Electronic Document Management System (desirable)
- Microsoft Office products and Visio (desirable)
- Scanner software (desirable).

Additional Record Capture Components will be written at a later date for other originating systems. These additional components do not fall within the scope of this tender.

The Encapsulation component is tightly coupled to the RKS and may be viewed either as a front end to the RKS, or a component within the RKS. It contains the functions that are commonly required when constructing VEOs. These include:

- Checking of metadata and entry of additional metadata
- Conversion of the captured content to preservation formats
- Allocation of a unique record identifier
- Allocation of the record to a folder within the RKS
- Actual construction of the VEO
- Application of digital signatures.

A key component of this tender is the design, implementation, and documentation of an interface between the Record Capture Components and the Encapsulator. This interface will be used in the future to develop new Record Capture Components for additional originating systems.

A diagram detailing different options for record creation can be found in **Part A – Annexure G – Figure 18 : Options for Record Construction.**

3.1.2 Record Capture Components

The capture function is achieved when the documents and their associated metadata that comprise the record, are obtained from the system that originally created these documents. The Record Capture components may be integrated into the RKS, or may be separate components. There is a need to capture records both on an individual basis and in bulk.

Different desktop and computer applications, as well as the file system, will be interfaced to the RKS for the capture of records. The desktop applications include word processors, spreadsheet packages, simple drawing tools, and electronic mail. The computer applications include Electronic Document Management Systems, workflow systems, transaction-based application systems, and information-based applications. In future implementations, other non-printable type electronic objects (e.g. sound files) will also need to be captured. Initially these types of objects will be captured directly from the file system.

These various systems are called originating systems in this specification. The originating system will be the source of the documents to be captured together with whatever metadata that could be automatically extracted from the environment.

The ability to automatically create metadata will vary among the originating systems. The computer application systems will probably provide the most complete metadata as the documents are used for a very specific, well-defined purpose. In contrast documents produced from native desktop applications and the file system will contain very little metadata. In these cases the users may need to be prompted to supply mandatory metadata fields.

The originating systems will be able to supply the record content in a variety of data formats. Some originating systems will be able to supply the document in long term preservation formats such as PDF, but in other cases the relevant Capture component will need to translate the document into an appropriate long-term format such as PDF. In the case of some non-printable type electronic objects there may be no appropriate long-term format, in which use the content will be captured in the original format only.

It is expected that there will be many different approaches to integrating the Record Capture component software into the desktop environment. These include:

- Part of the desktop application. In this scenario the desktop application would call the RKS and the Encapsulator software directly to generate VEOs.
- As a plug-in to the desktop application. In this scenario, the Record Capture component is a separate program to the application. The application would be extended to invoke the Record Capture software (e.g. using Visual Basic invoking ODMA).
- As a daemon. In this scenario, the Record Capture component is a separate program that is continuously running in the background. The application will signal the record capture process when it has a new native format record to capture, register and encapsulate.

- As a separate program. In this scenario, the Record Capture component is a stand-alone program specifically invoked by the user (e.g. by an icon) when it is necessary to capture a record.

3.1.3 Encapsulator

The function of the Encapsulator is to contain the functions that are common to the production of all VEOs. The Record Capture component interfaces the Encapsulator to the specific originating system via a defined application programming interface (API).

Although the Encapsulator is expected to contain common functions, this does not mean that all functions will be used by all Record Capture systems. For example, the Encapsulator could provide a function to allow a user editing of captured metadata, but this function need not be used by all Record Capture systems.

A record may consist of multiple documents, each of which may be represented by multiple encodings. For example, a record of this Request For Tender (RFT) would consist of four documents (Parts A to D), each of which may be represented by both a PDF and a Word file. This would result in eight content files being exported to the Encapsulator. Note that there will be 13 pieces of metadata associated with this record:

- 1 piece containing the metadata for the record as a whole,
- 4 pieces containing the metadata for the 4 documents; and
- 8 pieces containing metadata about each of the encodings.

The conceptual process of creating a VERS Encapsulated Object (VEO) is as follows:

- The metadata is checked for completeness and accuracy.
- A unique record identifier is assigned to the record.
- The information is expressed in the correct XML format.
- The VEO is, optionally, signed by the user creating the record.
- The Encapsulator signs the VEO.
- The VEO is stored by the RKS for preservation.
- The Encapsulator confirms to the Record Capture System (and hence the originating system) that the RKS has taken responsibility for the record. Metadata may be passed back to the originating system as part of this confirmation.

An illustration of this can be found in **Part A – Annexure G – Figure 6: Functions of Encapsulation.**

3.1.3.1 Digital Signatures

The Encapsulator always signs a VEO. In addition, the Encapsulator may sign the VEO on behalf of the user.

The Encapsulator will sign and date the VEO using its private key. Management of the Encapsulator's private key is described in the Signature Management component (see section 8.2).

The Encapsulator will also have the option of signing the record with the user's private key. This key is to be passed to the Encapsulator via the originating system and the Record Capture system.

Note that the application that originally created the document may have separately applied digital signatures to the document prior to the document becoming a record. For example, a workflow system may apply a digital signature to a document as part of an authorisation process. These separate digital signatures are not considered within the VERS RKS, but it expected that these application digital signatures would be stored as a separate document within the record. Note that the application digital signatures would depend on either using an external PKI, or on including appropriate certificate within the record.

The design of the Encapsulator is to support the following future extensions:

- The use of an independent Notary service. The Notary service will be passed a hash value of the VEO and will return a digital signature and time stamp.
- Access to the user's private key independently to the application (e.g. direct access via a file or a smart card).

3.1.4 Record Capture / Encapsulator API

Over time, it is expected that further originating systems will be interfaced to the Encapsulator to allow the capture of records from those systems.

Consequently, a critical part of this tender is the design, implementation, and documentation of an API to the Encapsulator. This API will be used to allow future Record Capture components to interface to the Encapsulator developed as a result of this tender.

As part of the RKS, the tenderer will develop a suitable API for use by originating systems.

A formal set of interface documentation is required to be produced. The target audience of this documentation will be programmers who have the task of interfacing applications to the Encapsulator.

3.1.5 Bulk creation of record VEOs

On occasions it will be necessary to create records in bulk. For example, all of the electronic mail stored within a particular "email folder" may be converted in one operation to records stored within a folder.

Two types of bulk creation are required. In the first type, all records created will be attached to the same folder. The particular folder will need to be selected by the user. An example of this type of creation is the capture of electronic mail messages that have been stored in internal "email folders".

In the second situation, the application producing the bulk records will already 'know' the folder that the records are destined for. The records may be for different folders. In some cases the loading of bulk records will require the creation of new folders according to the metadata supplied by the originating system. An example of this type of originating system is an Electronic Document Management System.

3.1.6 RKS creation of records

In addition to the creation of normal records, the RKS will create records to support its internal operation. These records will include:

- Certificate Records. These are records that contain the public key certificates used to verify the digital signatures applied to records within the RKS.
- Onion Records. These are generated when users modify the metadata associated with an existing VEO.

3.1.7 Requirements for Record Creation of VEOs

The RKS must allow electronic documents arising in the course of business to be captured as electronic records by an end user, by providing:

- facilities for the capture of electronic documents directly from the file system
- integration with common desktop applications such as Word, Excel, PowerPoint, VISIO
- integration with Lotus Notes, and the departmental EDMS
- capture of Web pages with all components
- capture of scanned paper documents
- an API (Application Programming Interface) to allow future integration with other applications.

The RKS must capture electronic records as Record VEOs (VERS Encapsulated Objects).

The RKS must:

- prevent any changes to the content of the electronic record
- prevent any changes to the metadata of the electronic records (except where specified)
- maintain electronic record content and metadata together in a tightly-bound relationship, once record capture has been initiated.

3.1.7.1 Mandatory requirements

B3.1 The RKS must capture records as VERS Encapsulated Objects (VEOs), formatted in accordance with PROV Standard PROS 99/007.

B3.2 The RKS must be able to allocate a unique identifier to each electronic record on registration, which serves to identify the unique record from the point of registration throughout the remainder of its life. The identifier must be unique within DOI.

B3.3 The RKS must be capable of capturing one or more electronic objects from the (computer) file system and converting them to a VEO.

The user will invoke the capture. The user will specifically identify electronic objects files to be included in the record, for example using a 'file open' type dialog box. Each selected object file will be preserved as a separate document within the one record.

The record metadata will, as far as possible, be captured from the system. The user will need to nominate the folder for the record and complete all mandatory metadata.

The records will be signed by the system creating the record (and not by the user creating the record).

B3.4 As a minimum, the RKS must be able to capture the following types of electronic objects from the file system:

- Microsoft Word 97 (and later) documents
- Microsoft Excel 97 (and later) spreadsheets and charts,
- Microsoft PowerPoint 97 (and later) presentations
- Microsoft Project 98 (and later) plans and charts
- Visio 5 (and later) diagrams
- Text files
- HTML and XML objects
- Image files such as tif, gif and jpeg.

B3.5 The RKS must interface to Lotus Notes R5 (and later) to allow the capture of a **single** electronic mail message and its conversion to a VEO. This includes simple electronic mail messages and electronic mail messages with attachments.

The user hitting an 'archive' button on the Lotus Notes toolbar will manually invoke the capture and conversion.

The record content will be the Lotus Notes document currently displayed, including all header graphics, metadata, and footer information. Sections in the document will be expanded. The captured document will form the first document within the captured record. Attachments will be captured as the second and subsequent documents within the record. Information about embedded document links will need to be included.

The record metadata will, as far as possible, be captured from the system or Lotus Notes. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

The record will be signed by the system creating the record (and not by the user creating the record).

B3.6 The RKS must interface to Lotus Notes R5 to allow the **bulk** capture of electronic mail from Lotus Notes mail folders. Each document is to be converted to a VEO. This includes simple electronic mail messages, and electronic mail messages with attachments.

The capture and conversion will be manually invoked by selecting documents in a Lotus Notes mail folder and hitting an 'archive' button on the Lotus Notes toolbar. Each selected document will be captured and converted to a separate VEO.

The record content will be a Lotus Notes document, including all header graphics, metadata, and footer information. Sections in the document will be expanded. The captured document will form the first document within the captured record. Attachments to the document will be captured as the second and subsequent documents within the record. Information about embedded document links will need to be included.

The record metadata will, as far as possible, be captured from the system or Lotus Notes. The RKS will *not* prompt the user to enter metadata for each record individually. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

The records will be signed by the system creating the record (and not by the user creating the record).

B3.7 When capturing electronic mail, the RKS must ensure the capture of electronic mail transmission data and be capable of mapping this data to electronic record metadata. Depending on the text and interpretation of the Electronic Transactions (Victoria) Act 2000, it may be necessary to capture email acknowledgments before creating the record.

B3.8 The RKS must ensure that the created VEO is signed by the system immediately upon creation.

B3.9 The RKS must capture the content of an electronic record both as a PDF file (or other approved long term preservation format) and in its native format.

B3.10 The RKS must ensure the capture of all mandatory metadata elements specified in the VERS metadata scheme (PROS 99/007 Specification 2) and any additional metadata specified by the system configuration, and retain them with the electronic record in a tightly-bound relationship at all times.

B3.11 The RKS must allow a record to be registered on multiple folders if required.

B3.12 The RKS must support the creation of relational links (e.g. 'see also' type links) between records of related interest.

B3.13 The RKS must be able to manage these relational links to ensure that:

- all references or pointers link to a valid destination
- change in location, e.g. renumbering, of a destination also redirects any linking references.

B3.14 The RKS must allow the definition of an unlimited number of additional structured metadata elements. These may be defined as sets of metadata associated with particular types of electronic records. The information associated with each new metadata element is:

- whether the new metadata element is defined as mandatory or optional
- whether the new metadata element is defined as repeating
- whether the metadata element may be modified by the user.

B3.15 The RKS must support the definition and application of validation rules for each type of metadata element, at a minimum including validation of:

- date formats
- numeric formats
- valid location in the Classification Structure.

B3.16 Where a controlled vocabulary or thesaurus controls metadata elements, the RKS must prevent the entry of terms not in the controlled vocabulary or thesaurus.

B3.17 The RKS must prevent any amendment to the content of any VEO.

B3.18 The RKS must allow the users to add/modify only specified metadata elements on the capture of the record. It must be possible to configure the metadata elements that may be modified by authorised users.

B3.19 The RKS must restrict the amendment of user-generated metadata to authorised users.

B3.20 The RKS must allow the allocation of an 'owner' to each record and folder. The owner has certain default rights to access the record and modify the metadata associated with it.

B3.21 The RKS must ensure that all electronic records are associated with one or more entries in the electronic Classification Structure on completion of capture.

B3.22 If a user has initiated the capture of the record, then the RKS must allow the user to allocate the record to a folder.

B3.23 The RKS must retain the original document title as part of the metadata and this element can be used for discovery, reporting and export purposes.

B3.24 The RKS must at all times prevent the deletion or loss of any electronic record that has been captured, with the exceptions of:

- Destruction in accordance with a disposal schedule
- Deletion by a Records Manager as part of an audited procedure.

B3.25 The RKS must be capable of taking an existing VEO and creating an additional layer of metadata around it to form an 'onion' VEO.

The user will invoke this function. The user will specify the VEO to encapsulate using the Discovery system.

The record content will be the original VEO.

The metadata will, as far as possible, be captured from the original VEO or the system. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

The VEO will be signed by the system creating the record (and not by the user creating the record).

B3.26 The RKS must provide an Application Program Interface to the Encapsulator and the API must have the following characteristics:

- A record will consist of one or more documents, and each document will consist of one or more encodings. Each record, document, and encoding will have metadata associated with it.
- A successful (non-error) return will indicate that the Encapsulator (or the Record Keeping System) has accepted responsibility for the preservation of the record and that the originating system can discard its copy.
- The API must operate in either synchronous or asynchronous modes. Synchronous mode means that the Encapsulation request will not return until the constructed VEO is accepted by the Record Keeping System. Asynchronous mode means that the Encapsulation request will return immediately, and success or failure of the encapsulation must be determined by a subsequent call to the Encapsulator.
- The Encapsulator must be capable of returning metadata to the originating system via the Record Capture components. The originating system or Record Capture component will use this metadata as the basis for subsequent linked records. The Record Capture component will request specific metadata fields to be returned, and only those fields will be returned.
- New Encapsulator functions, and new arguments to existing functions, must be easily added without requiring modifications to existing Record Capture components that use the API.
- It must be possible to extend the metadata associated with a VEO without requiring modifications to Record Capture systems that do not use the new metadata elements or the API.
- Every API response (whether signalling a normal return or an error) is to contain a number that distinguishes it from all other types of response. Numbers assigned to errors are to be easily distinguished from numbers assigned to normal returns. In addition, each response is to contain a text message describing the response (the message would be used as an error prompt presented to the user). The text message should be meaningful to the user, and must clearly state whether the record was successfully created in the RKS or not.

- If convenient, metadata may be passed between the Record Capture component and the Encapsulator as XML fragments.

B3.27 The documentation of the Encapsulator API is to include the following:

- An orientation overview that describes how the interface is used and the relationship of the various function calls.
- Detailed function specifications. Each specification is to describe the arguments passed to it, and results returned, in detail. The data structures passed and returned are to be described in detail. All possible errors are to be listed and the causes of the error explicitly listed.
- Annotated examples of the use of the interface.

3.1.7.2 Desirable requirements

B3.28 The RKS Encapsulator should provide a standard metadata entry form that can be invoked by applications when it is necessary for users to enter metadata.

B3.29 If the record capture is an automated process, then the rules governing the allocation of the record to a folder will need to be defined as part of the automated process. In some cases the automated process may trigger the creation of a new folder before allocating the record.

B3.30 The RKS should interface to Lotus Notes R5 (and later) to allow the capture of a **single** Lotus Notes document and its conversion to a VEO. These include outgoing facsimile messages, outgoing facsimile messages with attachments, and other documents from other Notes databases such as teamrooms and knowledge bases.

The user hitting an 'archive' button on the Lotus Notes toolbar will manually invoke the capture and conversion.

The record content will be the Lotus Notes document currently displayed, including all header graphics, metadata, and footer information. Sections in the document will be expanded. The captured document will form the first document within the captured record. Attachments will be captured as the second and subsequent documents within the record. Information about embedded document links will need to be included.

The record metadata will, as far as possible, be captured from the system or Lotus Notes. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

The record will be signed by the system creating the record (and not by the user creating the record).

B3.31 The RKS should interface to Lotus Notes R5 to allow the **bulk** capture of a number of Lotus Notes documents from a database. Each document is to be converted to a VEO. These include outgoing facsimile messages, outgoing facsimile messages with attachments, and other documents from other Notes databases such as teamrooms and knowledge bases.

The capture and conversion will be manually invoked by selecting documents in a Lotus Notes database and hitting an 'archive' button on the Lotus Notes toolbar. Each selected document will be captured and converted to a separate VEO.

The record content will be a Lotus Notes document, including all header graphics, metadata, and footer information. Sections in the document will be expanded. The captured document will form the first document within the captured record. Attachments to the document will be captured as the second and subsequent documents within the record. Information about embedded document links will need to be included.

The record metadata will, as far as possible, be captured from the system or Lotus Notes. The RKS will *not* prompt the user to enter metadata for each record individually. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

The records will be signed by the system creating the record (and not by the user creating the record).

B3.32 The RKS should be capable of capturing the associated embedded document links when capturing the content of a Lotus Notes document. Notes documents include simple electronic mail messages, electronic mail messages with attachments, outgoing facsimile messages, outgoing facsimile messages with attachments, and other documents from other Notes databases such as teamrooms and knowledge bases. The record content will include the Notes document as the first document within the record.

The user will invoke this function to capture the embedded links and nominate which documents linked by embedded links are to be included in the records. Linked documents may be other Notes documents, web pages, or links to documents held within the Electronic Document Management System.

Other documents linked to the Notes document are to be displayed and the user will need to confirm the capture of this displayed content as another document within the record. Any web pages within the link page are also to be displayed for the user to confirm the capture of the content as another document in the record.

The user must be able to indicate that they do not want to continue following any more embedded links and return to the original Notes document.

The metadata will as far as possible be captured from the original Notes document or the system. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

B3.33 The RKS should provide integration with common desktop applications (Microsoft Office 97 and later versions, and Visio 5 and later versions) to allow capture of the document as a record and conversion to a VEO. The user must invoke the Record Capture. Each document will be preserved as a document within the one record. The record metadata will, as far as possible, be captured from the desktop applications. The records will be signed by the applications creating the record (and not by the user creating the record).

B3.34 The RKS should be capable of creating VEOs from scanned images.

A user will invoke this function.

The record content will be a scanned image (or series of scanned images). The images may be subject of Optical Character Recognition. Multiple encodings (formats) may be captured into the record, but one encoding must be PDF.

The metadata will, as far as possible, be captured from the system. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

The records will be signed by the system creating the record (and not by the user creating the record).

B3.35 The RKS should interface to Lotus domino.Doc (versions 2.5a and later), used as an Electronic Document Management System at DOI, to allow the capture of documents from the EDMS. Each such document is to be converted to a VEO.

The RKS will be automatically invoked by the EDMS. The system must be configurable for the record creation process to be mandatory or at the option of the user.

The record content will be the checked-in document. This will form the first document within the captured record. Any attachments will be captured as the second and subsequent documents within the record.

The metadata will, as far as possible, be captured from the system or the EDMS. In particular, if a previous version of the document has been captured as a record, the metadata should be sourced from the previous version. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

The records will be signed by the system creating the record (and not by the user creating the record).

B3.36 The RKS should be capable of capturing the content of Web pages.

The user will invoke this function. The user will specify the URL of the page to encapsulate.

The record content will be a Web page; this will form the first document within the record. Any component of the Web page contained wholly within the Web page (e.g. an image) should be captured within the record. Note that this does not guarantee capture of linked Web pages, nor capture of Web objects whose URL is 'hidden' on the page (e.g. embedded within scripts or code). Such capture of ‘hidden’ objects is beyond this initial system.

The metadata will, as far as possible, be captured from the Web page or the system. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

The records will be signed by the system creating the record (and not by the user creating the record).

B3.37 The RKS should be capable of capturing the associated embedded links when capturing the content of a web page.

The user will invoke this function and nominate which documents linked by embedded links are to be included in the records.

The user will specify the URL of the page to encapsulate.

The record content will be a web page, this will form the first document within the record.

Other web pages linked to the page are to be displayed and the user will need to confirm the capture of this content as another document within the record. Any web pages within the link page are also to be displayed for the user to confirm the capture of the content as another document in the record.

The user must be able to indicate that they do not want to continue following any more embedded links and return to the original web page.

The metadata will as far as possible be captured from the web page or the system. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

B3.38 The RKS should ensure the capture of an 'intelligent' version of an electronic mail message address (where one is associated with the original message) for example, *'John Smith'* rather than *js042@aol.com*.

B3.39 In addition to those specified in *Mandatory Requirement B3.4*, the RKS should be able to ensure the capture as VEOs of, and manage, the following types of electronic documents which have been created or received in the course of business:

- office documents with embedded objects from a different package, for example a word processing document with embedded spreadsheet
- databases created in desktop office application packages
- digital video clips
- electronic diaries and notepads
- physical data files from CAD/CAM applications
- digital maps and plans
- digitised sounds.

B3.40 The RKS should be capable of assigning to each electronic record a sequence number which is unique within a specified level of the classification structure; use of this number to be selectable at time of implementation. Note that this sequence number is different to the unique identifier discussed under the mandatory requirements.

B3.41 The RKS should be able to link an instance of an electronic record (that is, a redaction of the original record from which portions of content have been masked) to the original record, so that retrieval of one allows retrieval of the other, whilst retaining separate metadata and access controls over the two items.

B3.42 The RKS should support the signing of a VEO by a private key held by the creator of the record. This includes ensuring the preservation of the necessary certificates to subsequently authenticate the digital signature.

B3.43 The RKS should support the use of a notary service to sign and date VEOs independently of the RKS.

B3.44 The RKS should provide support for decisions on the allocation of electronic records to electronic folders by:

- suggesting the most recently used folders by that user
- suggesting folders which contain known related electronic records
- suggesting folders by inferences drawn from record metadata elements: for example, significant words used in the document title.

B3.45 The RKS should allow an end user to pass electronic records to a Records Manager In-tray during the process of registration, to complete the process by classification within the classification structure.

3.2 Record Creation Process for Paper Records

Paper records will be managed along side related electronic records in the same Folder. There will not be separate paper and electronic folders of records. Paper records belonging to the same Folder will be bound together with a paper file cover. This cover is **not** the Folder but merely a means to organise the paper records. The location of the paper file cover and the attached paper records will need to be managed by the RKS.

Part A – Annexure G – Figure 12 : Folders and Paper Records shows a diagrammatical representation of the relationship among paper documents, paper file covers, and the RKS electronic Folder.

3.2.1 Requirements

3.2.1.1 Mandatory Requirements

B3.46 The RKS must allow paper records to be registered by the user. The user will need to nominate the folder for the record and complete all mandatory metadata. One of the metadata fields will be the location of the paper file cover to which the paper record is physically attached. Information about the physical location of the paper records must be stored as a field on the Folder. Paper records do not have to be represented in the RKS as VEOs, but will need to be converted to VEOs at the time of Export to another system, (the main difference will be that the document content will be empty).

3.2.1.2 Desirable Requirements

B3.47 If a paper record, already registered in the RKS, is subsequently scanned, the RKS must allow for a scanned image of a paper record, to be 'inserted' into the document content area of the record, and the metadata completed to reflect the addition of the scanned image to the record. It is desirable to create a VEO if all documents in the record have been scanned.

4. Import/Export of Records/Folders

The import/export function allows records managers to export custody of records and folders (and the records they contain) from one VERS Record Keeping System to another VERS Record Keeping System. This may occur due to the export of functions from one Agency to another, the export of records from one Record Keeping System to its replacement, or the export of records to PROV. Export occurs either on demand or after the disposal process.

The records contained within the exported folders must have complete VEO information, including a full history. If the RKS does not record changes to metadata as onion layers around the VEO as they occur, then the changes recorded in the RKS will need to be applied to the VEOs before they are exported.

Folders and the records they contain may either be exported using the Victorian Government Intranet or export media as defined in the PROS 99/007 standard (e.g. CDs). The RKS will need to have the capability of encrypting the VEOs as they are exported to ensure that sensitive documents are not exposed in the process.

An illustration of this can be found in **Part A – Annexure G – Figure 7 : Export for Transfer Functions & Process**, as well a diagram on transfer to PROV Archive can be found in **Part A – Annexure G – Figure 19 : Options for VEO Construction to PROV Archive.**

4.1 Export of Records

The RKS must be able to export folders and the records they contain. Records (electronic and paper based) will be exported as Record VEOs, and folders as File VEOs.

The export function must check and (if necessary) update the metadata associated with a VEO (e.g. update the Agency if this has changed since the VEO was created). It must also add an entry in the management history of the VEO documenting the export. This modified metadata will form an additional layer of metadata around the original VEO.

The functions to be provided by the Export module are:

- Select records to be exported
- Extract record keeping metadata, such as management history and other selected information, to include as an onion layer around the record VEO
- Export records – ensuring that the Agency identification and other information is up to date
- Store information about the export in the RKS
- Export the folder information as a File VEO
- If necessary, allocation of series when exporting to PROV
- If necessary, export the certificate records that will allow the importing RKS to verify the digital signatures used to sign this record.

4.1.1 Requirements for Export of Records

4.1.1.1 Mandatory requirements

B4.1 The RKS must restrict access to the Export function to Records Managers or nominated staff.

B4.2 The RKS must be able to support the flagging of electronic folders and groups of folders for export to another VERS RKS, or for export to Public Record Office Victoria.

B4.3 The RKS must be able to identify and list electronic folders marked for permanent preservation as their disposal schedules come into force.

B4.4 The RKS must export records as VERS Encapsulated Objects (VEOs) encoded according to PROV Standard PROS 99/007.

Where metadata associated with a record has been modified or augmented after capture, the RKS may wrap the modified metadata around the original record to form an onion layer upon export. It is not necessary to continually create onion layers as the metadata is modified.

B4.5 The RKS must export folders and folder parts as File VEOs (VERS Encapsulated Objects) according to PROV Standard PROS 99/007.

B4.6 The exporting RKS must document each export within the folder. This documentation is to include: the current date and time; the titles and identifiers of all records exported; and the identity of the importing RKS, including the owner of the system and its network name/address (if the importing RKS is on the network). This information must be documented using defined metadata elements.

B4.7 The RKS must confirm that the destination system has the necessary certificate records to be able to validate all the digital signatures associated with the exported VEOs. If not, the RKS must copy the necessary certification records to the destination system.

B4.8 The RKS must be able to export a record that occurs in multiple folders; at a minimum, through physical duplication of the record to be exported.

B4.9 The RKS must produce a report detailing any failure to export electronic records and folders, and identifying the records allocated for export which have generated processing errors.

B4.10 The RKS must retain all electronic folders that have been exported or exported intact (including the records they contain), until the importing system confirms that the folders and records have been accepted.

B4.11 Export between two VERS systems should be possible either directly on-line or by physical export of media. The RKS must provide functionality for the Records Manager to manage the export to physical media at an operational level, and to manage the resulting physical media.

B4.12 The RKS must be capable of exporting information about paper records as VEOs.

B4.13 The RKS must provide the ability to:

- add user-defined metadata elements required for archival management purposes to electronic folders selected for export
- sort electronic folders selected for export into ordered lists according to user-defined metadata elements
- generate user-defined forms to describe electronic folders that are being exported.

4.1.1.2 Desirable requirements

B4.14 The RKS should be able to identify and report on electronic records to be exported, which transgress the following conditions:

- where a record or folder marked for export references (i.e. points to) a record or folder which is not so marked
- where a record or folder marked for export is referenced (i.e. is pointed to) by a record or folder not so marked

and enable the conflict to be resolved by:

- retaining a copy of the destination record within the folder
- creating a fresh copy of the destination record and re-directing all linking references
- removing all linking references with the destination record.

B4.15 Where the RKS wraps changed metadata as an 'onion' layer around the original VEO upon export, the RKS should enable selection of the folder and record metadata added, and should only add that set of metadata.

B4.16 The RKS should be able to export records located in more than one folder without duplication of records.

B4.17 The RKS should be able to export the classification structure associated with the exported records.

B4.18 The RKS should allow exported records to remain within (and not be deleted from) the system at the option of the Records Manager.

B4.19 The RKS should be able to encrypt the exported record VEOs and File VEOs. The Records Manager must be able to configure whether exported record VEOs and File VEOs are encrypted.

B4.20 When exporting over the Internet, the VERS RKS must be capable of exporting records using SSL (Secure Socket Layer) 3.0. The SSL implementation must provide a range of cipher suites conformant with SSL 3.0. Tenderers should state what cipher suites will be supplied in **Part D: Tender Form and Vendor Response Schedule 8.10**.

B4.21 The VERS RKS should be capable of exporting records, other than over the Internet, encrypted using the same cipher suites as used with SSL 3.0.

4.2 VEO Import

The RKS must be able to import records and folders as Record VEOs and File VEOs.

The import function will need to verify that the metadata on the incoming VEOs is correct and add an 'onion layer' to reflect the importing Agency's details. Some re-classification of the records may be necessary to comply with the RKS classification in the receiving Agency.

The functions to be provided by the Import module are:

- Review the records to be imported and select records to be imported
- Create folder(s) to store imported records
- Associate Record VEOs and File VEOs with relevant folders
- Verify that the metadata is complete on records to be imported
- Verify all digital signatures on records to be imported
- Where a File VEO is associated with a folder in the importing RKS, require the ability to select the information to be imported from the File VEO to the folder. The actual File VEO is converted to a record and placed on the folder (to document the former history of the file on the original RKS).
- Allow the Records Manager to add comments and additional metadata to the imported record. For example, it may be necessary to accept a VEO with an invalid signature, but this will be documented by a comment in the management history of the record.

A diagram on VEO Import can be found in **Part A – Annexure G – Figure 9 : Import VEOs Functions & Process.**

4.2.1 Requirements for VEO Import

4.2.1.1 Mandatory Requirements

B4.22 The RKS must restrict access to the Import function to Records Managers or nominated staff.

B4.23 The RKS must be capable of importing folders (and the records they contain), and records from another RKS (this is the counterpart of the export function).

B4.24 The RKS must be capable of associating imported records and folders with folders in the importing RKS.

B4.25 The RKS must create a new folder for each new imported folder. The metadata associated with the new folder is to be based on the metadata contained in the imported File VEO, but can be modified by the Records Manager controlling the importing RKS (e.g. to allow for the reclassification of the folder). The File VEO is to be converted to a record and filed within the folder.

B4.26 The RKS must document the import within the folder using defined metadata elements. This documentation is to include:

- the current date and time; the titles and identifiers of all records imported; and
- the identity of the exporting RKS, including the owner of the system and its network name/address (if the exporting RKS is on the network).

B4.27 The RKS must check that the import of a VEO was without error and, if necessary, automatically invoke a re-import. The system must be capable of dealing with an interrupted import (due to failure of the network or importing RKS).

B4.28 The RKS must be capable of accepting VEOs that are an extension to PROS 99/007 (i.e. contain metadata elements that are not specified by that standard). The RKS must not discard information from such VEOs, and it must support searching and display of the information.

B4.29 The RKS must verify that each VEO conforms to PROS 99/007. VEOs that fail this test are to be brought to the attention of the Records Manager who will have the option of accepting or rejecting the import of the VEO. If the VEO is missing mandatory metadata but is accepted, the fact of the incomplete metadata is to be documented in the VEO's management history.

B4.30 The RKS must verify all digital signatures on imported VEOs, including the signatures on any internal metadata layers. VEOs with digital signatures that cannot be verified (because of missing certificates) and VEOs with invalid signatures are to be brought to the attention of the Records Manager. If the VEO is accepted, the fact of the unverified or invalid signature must be able to be documented in the VEO's management history.

B4.31 The RKS must confirm successful import of the folder when the File VEO and all record VEOs have been accepted. If any of these record VEOs are rejected, the import of the entire folder fails and the folder is removed from the importing RKS. Once the confirmation of import has been sent, the importing RKS is responsible for the preservation of that folder and the records it contains.

B4.32 The RKS must confirm successful import of any individual records when the record VEO has been accepted. Once the confirmation of import has been sent, the importing RKS is responsible for the preservation of that the record.

B4.33 The RKS must be able to import Certificate Records.

B4.34 The RKS must allow a Records Manager to review an imported folder to delete unwanted records. Full details of each deleted record must be able to be recorded in the folder's management history, including details of the Records Manager who authorised the deletion.

B4.35 When importing over the Internet, the VERS RKS must be capable of importing records using SSL (Secure Socket Layer) 3.0. The SSL implementation must provide a range of cipher suites conformant with SSL 3.0. Tenderers should state what cipher suites will be supplied.

B4.36 The RKS must be capable of importing information about paper records as if they were VEOs.

B4.37 The RKS must be capable of importing VEOs via both on-line and off-line (import of physical media).

4.2.1.2 Desirable Requirements

B4.38 The RKS should be capable of automatically reclassifying imported folders and modifying metadata according to a pre-defined plan.

B4.39 The RKS should be able to import a classification structure and use this to extend the classification structure managed by the RKS.

B4.40 The RKS must be able to import a complete set of VEOs, from another Agency or Department, and automatically recreate the classification structure, security, etc.

B4.41 The RKS should be capable of automatically extending the metadata managed by the RKS to handle extensions to PROS 99/007 used by imported VEOs.

B4.42 The VERS RKS should be capable of importing records, other than over the Internet, encrypted using the same cipher suites as used with SSL 3.0.

5. RKS Records Management Functions

The RKS will need to offer similar functionality to that provided in traditional Records Management systems. While there are functions that are relevant only to electronic or paper records, most of the requirements are common to both types of records.

Records Management functionality includes:

- The definition and on-going maintenance of corporate classification structures
- The establishment and application of corporate disposal schedules in line with PROV guidelines
- The implementation of appropriate security mechanisms to restrict access to folders and records as appropriate (see section 9)
- The creation and management of folders to which records are allocated
- The management of records stored in the RKS
- Audit log of changes made to folders and records in the RKS (see section 9)
- Tracking of paper records and covers
- Reporting and statistical analysis (see section 7)

Most of the functional requirements above are detailed in this section, but some functions, such as security, audit and reporting are covered in later sections.

The diagram in **Part A – Annexure G – Figure 10 : Records Management Functions** shows all the functions discussed in this section.

5.1 General Records Management

This section details the functionality that is common for both paper and electronic records management.

Folders are used as the method of grouping related records together. Folders must be created in the RKS and allocated the correct classification, disposal schedule, security, descriptive abstract, unique identifier, and a range of other metadata. Records are allocated to folders at the point of record capture, and inherit the characteristics defined for the folder, e.g. classification, disposal schedule and security.

Most of the management functions are applied at the folder level and affect all records attached to the folder. Folders may have multiple parts, but these are essentially distinct folders with similar characteristics to the main folder. Further details about part folders may be found in section 5.1.4 *Folder Management*.

Both paper and electronic records management revolve around folders, with the folders being common in format for both types except for additional bar-code and physical location details for folders containing paper records. A folder can contain both electronic and paper records. Electronic records are encapsulated including the record content and associated metadata. For paper records, only the record metadata is held in the RKS.

It should be noted that electronic records will be held in the RKS as VEOs, but folders created in the RKS will not be encapsulated into File VEO format until they are exported. Refer to section 4 *Import/Export* for further details. Likewise the metadata for paper records will not be encapsulated until the records are exported.

5.1.1 Classification Structure

The RKS will require a classification structure to enable the organisation of folders and records into meaningful groups. The hierarchical classification structure should reflect and support the business activities of the Agency. The same classification structures should be applicable to both electronic and paper records. Multiple classification structures are desirable to support the multiple Agencies within DOI.

Folders will be classified when they are created in the RKS. Records will be classified at the point of capture when they are associated with a folder.

Government Agencies are frequently re-organised and business units re-structured. The classification structures must be able to be modified to accommodate these changes and allow the re-classification of the RKS folders without major re-organisation of the folders, while maintaining an audit log of previous classifications.

The classification structures will also be used to assist searchers as a reference map, or finding aid, to locate the information they are looking for.

The RKS classification structures must:

- Provide consistent and predictable structuring principles, including at least a five-level hierarchical structure.

- Support both a numerical coding and a text-based naming convention.
- Incorporate:
  - Functional Groups (service and output)
  - Multiple levels of classification
- Allow the classification of a record by multiple entries within the structure and must then manage the referential integrity of all index data.

5.1.1.1 Mandatory requirements

B5.1 The RKS must support a classification structure, consisting of electronic folders and electronic folder parts. Electronic records must be classified to one or more folder parts during the capture and encapsulation process. Paper records must be registered to one or more of the folder parts.

B5.2 The RKS must support a hierarchical classification structure, with a configurable number of levels (a minimum of five (5) levels) below the root level excluding the folder level. An example would be

- Level 1 – DOI
- Level 2 – Business Unit
- Level 3 – Broad level subject heading
- Level 4 – Narrower subject heading
- Level 5 – Specific subject heading
- Folder

B5.3 The RKS must support the management of the classification structure, including the addition of new terms, the deletion of existing terms, the renaming of terms, and the relocation of terms within the tree. Note that deletion, renaming, or relocation of existing terms may affect folders and records within the RKS.

B5.4 The RKS must be capable of limiting the use of the functions that manage the classification structure to Records Managers.

5.1.1.2 Desirable requirements

B5.5 The RKS should support multiple classification structures.

5.1.2 Thesaurus

A thesaurus is a structured list of values with links between broader, narrower, and related terms.

5.1.2.1 Mandatory requirements

B5.6 The RKS must support the association of a thesaurus with any metadata element.

B5.7 It must be possible for thesauri to be held externally to the RKS.

B5.8 The RKS must support the management of a thesaurus, including the addition of new terms, the deletion of existing terms, and the management of relationships between terms.

B5.9 The RKS must be capable of limiting the use of the functions that manage a thesaurus to Records Managers.

5.1.3 Controlled Vocabularies

A controlled vocabulary is a simple list of valid terms or values.

5.1.3.1 Mandatory requirements

B5.10 The RKS must support multiple controlled vocabularies, potentially one for each metadata element.

B5.11 The RKS must support the association of a controlled vocabulary with any metadata element. It is preferable that the allocation of a value is via a drop down list taken from the controlled vocabulary in question.

B5.12 The RKS must allow the specification of the values for each controlled vocabulary.

B5.13 The RKS must allow the specification of a default value for each controlled vocabulary.

B5.14 The RKS must support the management of each controlled vocabulary, including the addition of new values, the deletion of existing values.

B5.15 The RKS must be capable of limiting the use of the functions that manage controlled vocabularies to Records Managers.

5.1.4 Folder Maintenance

The RKS will need to allow the creation and maintenance of folder details:

- Creation of new folder (and subsequent part folders)
- Modification of folder details such as title, classification, etc.
- Closure of folders
- Deletion of folders – this to be possible only by the Records Manager. (Users requesting folder deletion would have to send the request to the Records Manager's in tray)
- Audit trail of changes made
- Archival details of folders which contain paper records

5.1.4.1 Mandatory requirements

B5.16 The RKS must provide at least two naming principles for electronic folders:

- a mechanism for allocating a structured numerical reference code to each electronic folder

- a mechanism to allocate a textual folder title for each electronic folder.

Both of these principles can be separately applied in the same system.

B5.17 The RKS must ensure that the full path of the numerical reference and text name can uniquely identify each electronic folder.

B5.18 The RKS must allow the addition of electronic folders and record the date of the opening of the folder.

B5.19 The RKS must allow the addition of electronic parts to any electronic folder, which is not closed.

B5.20 The RKS must support the concept of open and closed electronic folder parts; only the most recently created part within a folder will be open and all other parts within that folder will be closed.

B5.21 The RKS must allow a folder to be renamed. There are two ways this can be done:

- Modify the metadata on the existing folder to reflect the changes necessary. This would be done when an error has been made in the metadata (e.g. spelling mistake, wrong information, etc).
- Create a new folder with the new information and then close the old folder, creating a relational link between the new and the old folder. This would be used when the nature of the folder has changed, but the old folder is still relevant (e.g. change of committee or organisation name, etc).

Entries will need to be made in the Management History of each folder reflecting the nature of the changes.

B5.22 The RKS must allow a folder or folder part to be closed to prevent the further addition of records or parts to that folder or folder part.

B5.23 The RKS must prevent the addition of records to a closed folder part.

B5.24 The RKS must allow a previously closed folder or part to be opened for the addition of records, and subsequently to close that folder or part again. This function should be restricted to Records Managers or people granted this level of access by the Records Managers.

B5.25 The RKS must allow a folder and its parts to be relocated to a different position in the classification structure, and must ensure that all records allocated to that folder and part remain so allocated following the relocation.

B5.26 The RKS must allow a record to be re-located to another folder part.

B5.27 The RKS must prevent the deletion of a folder and its contents at all times, with the exceptions of:

- destruction in accordance with a disposal schedule by the Records Manager.

- deletion by an authorised person within the RKS as part of an audited procedure.

B5.28 The RKS must support the use of folder level metadata. Amendments to folder metadata must be promptly propagated to the Discovery system so that new metadata can be searched and that old metadata is no longer visible to users.

B5.29 The RKS must allow a record to have multiple entries (i.e. the same record appears in multiple folders).

B5.30 Where multiple entries are achieved by use of a pointer system, the RKS must be able to manage the integrity of all pointers or references, to ensure that:

- all references or pointers link to a valid destination
- where a record has multiple entries, removal (by export or destruction) of one of the entries (links) does not result in removal of the record.
- change in location of a destination also redirects any linking references.

B5.31 The RKS must be able to link related folders. The types of relations allowed are to be configurable and allow the option of users defining their own relations. Back relations have to be automatically added. The RKS must support the creation of relational links (e.g. 'see also' type links) between folders of related interest.

B5.32 The RKS must be able to manage these relational links to ensure that:

- all references or pointers link to a valid destination
- change in location of a destination also redirects any linking references.

B5.33 The RKS must be capable of generating a document describing the folders and folder parts within the classification structure at any given instant. The objects described within this document are to be hyperlinked together so that clicking on a reference takes the user to the referenced object (using the Discovery system).

B5.34 When creating a new folder in a structure, which uses a structured numerical coding reference, the RKS should automatically generate the next sequential number available at that position within the structure.

B5.35 The RKS should support the ability to create multiple entries for electronic records in different electronic folders without physical duplication of the electronic record itself.

5.1.4.2 Desirable requirements

B5.36 The RKS should support an optional folder naming mechanism that is based on keyword list terms and relationships drawn from a thesaurus.

B5.37 The RKS should support the allocation of keyword list terms and relationships, as descriptive folder metadata subject terms in addition to the folder name and numerical reference code.

B5.38 The RKS should validate the name – numerical code or textual title – as it is allocated to a newly created electronic folder, according to specified validation rules.

B5.39 The RKS should be able to automatically close a folder part on fulfilment of specified criteria to be defined at configuration, including at least:

- parts delineated by an annual cut-off date; for example, the end of the calendar year, financial year or other defined annual cycle
- the passage of time since a specified event; for example, the last addition of a record to that part
- the number of electronic records which a part contains
- the physical size (in disk storage terms) of the electronic records contained in a part.

5.1.5 Record Maintenance

Once an object has been captured and encapsulated it becomes a VEO. Once a VEO has been registered into the RKS it is known as a record. Records need to be managed in a similar manner to the folders they reside in.

The RKS must provide the following functionality to effectively manage records:

- Maintain record metadata elements
- Associate related records with each other
- Create onion records from the audit trail.

5.1.5.1 Mandatory requirements

B5.40 The RKS must allow records to be associated with one or more folders.

B5.41 The RKS must allow records to be re-classified to another folder or added to multiple folders at the same time.

B5.42 The RKS must allow the modification of record metadata where necessary and record the changes in the appropriate audit log. Changes must be promptly promulgated to the Discovery system. The modifications in the audit log will eventually form an onion layer around the original VEO. This onion layer must be formed upon export (to ensure that the current metadata is exported), and can be formed upon demand.

B5.43 The RKS must be able to link related records. The types of relations allowed are to be configurable and allow the option of users defining their own relations. Back relations have to be automatically added.

B5.44 The RKS must allow the tagging of an individual record, or records, on receiving a Freedom of Information (FOI) request. The FOI Manager must be able to 'freeze' the record to stop any alterations to the metadata, prevent reclassification of the record, until the FOI request has been dealt with. Once the record(s) have been frozen, any access to the record is be 'read only', with the exception of the Records Manager and the FOI Manager.

B5.45 When the RKS wraps changed metadata as an 'onion' layer around the original VEO, the RKS should enable selection of the folder and record metadata added, and should only add that set of metadata.

B5.46 The RKS should provide the ability, on demand, to wrap changed metadata from the audit trail around a record to create an onion record.

B5.47 The RKS must be capable of taking an existing VEO and creating an additional layer of metadata around it to form an 'onion' VEO.

The user will invoke this function. The user will specify the VEO to encapsulate using the Discovery system.

The record content will be the original VEO.

The metadata will be captured from the original VEO, the audit log or the system. Time and date metadata must be obtained from a source that can not be modified by the user creating the record.

The VEO will be signed by the system creating the record (and not by the user creating the record).

5.1.6 Record Types

The RKS will capture different types of records from different sources, e.g. from different business units and from different capture systems. The record types will define the metadata fields relevant for the different types of records, including the mandatory fields that must be recorded.

The record types may be used by the Discovery system to assist the user looking for specific types of records. This will be of use for searchers familiar with the records and wishing to narrow down the search criteria. The user may specify particular fields relevant to the record type being searched (e.g. author, date range, etc).

The record types may also be used to define the sentencing policy for the records.

5.1.6.1 Mandatory requirements

B5.48 The RKS must support the ability to define different record types for electronic records. Examples of distinct types are:

- pre-defined forms
- committee minutes
- letters
- electronic mail.

B5.49 The RKS must allow the discovery and reporting on these record types.

B5.50 The RKS must support the definition of different metadata elements (beyond those defined in PROS 99/007) for each record type.

5.1.7 Disposal of Records

The disposal of records is performed at the folder level, not at the record level. Disposing or exporting a folder affects all the records within the folder. The export of a folder to another Agency is achieved by exporting the records and the folder as detailed in section 4. It is not possible to destroy individual records without destroying the folder, but it is possible to export individual records to another RKS.

Public Record Office Victoria sets disposal schedules for Departments. The disposal schedules are implemented as sets of disposal policies in a record keeping system.

The RKS must be capable of allocating a disposal policy to groups of folders and folder parts. The disposal policy will be initiated by time-based criteria, event-based criteria, or a combined time and event-based criteria, and will determine which disposition actions are to be taken on the folder or part to which it is allocated.

The RKS must support disposal policies that comprise:

- A specification of the folders that the policy applies to.
- The event that will trigger a disposal event. These triggers will be a particular date or an elapsed time after an event (creation of folder, addition of last record).
- The actions to be taken on folders that match the trigger event.
- A reference to the source of the policy (e.g. legislation).

A diagram on the destruction of records and storage media can be found in **Part A – Annexure G – Figure 8 : Export for Destruction Functions & Process.**

In addition to the disposal triggers described in this section, folders may also be sentenced if the folder contains paper records held in a box that is sentenced for disposal (see B5.102).

5.1.7.1 Mandatory requirements

B5.51 The RKS must enable disposal policies to be allocated at any point in the classification structure, including the folder or folder part. This disposal policy is to be inherited by the lower levels in the classification structure, folder, or folder parts, unless explicitly overridden by another disposal policy.

B5.52 The RKS must allow an addition of a new disposal policy to the Record Keeping System.

B5.53 The RKS must allow the modification of a disposal policy. Any of the information in a policy can be altered. Changes will not affect folders that have already been disposed.

B5.54 The RKS must allow the removal of a disposal policy.

B5.55 The RKS must enable a disposal policy to be allocated to a specific folder that can take precedence over a disposal policy allocated at a higher point in the classification structure for this folder.

B5.56 The RKS must allow the allocation of a separate disposal policy to an individual part within a folder; where an individual part is not allocated a distinct policy, the policy for the folder must come into force.

B5.57 The disposal policy must be applied to all of the records contained within the folder or folder part.

B5.58 The RKS must ensure that where a record has multiple entries in more than one electronic folder, and these folders have different disposal policies, the actual record will not be disposed of until the last disposal policy has been triggered.

B5.59 The RKS must support disposal policies which consist of:

- a retention period
- a set of disposition instructions
- reference to the approval authority (e.g. disposal schedule).

B5.60 The RKS must support the allocation of a retention period which can be expressed as:

- the passage of a period of time
- the occurrence of a specified event
- the passage of a period of time following a specified event.

B5.61 The RKS must support types of 'occurrence of a specified event' in a retention period which include:

- opening date of a folder or part
- closing date of a folder or part
- last addition of a record to a folder or part
- last retrieval of a record from a folder or part.

B5.62 The RKS must support types of 'occurrence of a specified event' in a retention period, which occurs outside the knowledge of the system, and must enable the Records Manager to record the fact that a specified event has occurred.

B5.63 The RKS must automatically track retention periods that have been allocated to electronic folders within the system, and initiate the disposal process once their specified conditions are fulfilled.

B5.64 The RKS must support the allocation of disposition instructions as part of a disposal policy which include:

- review of the folder and contents.
- export of the folder and associated records to another VERS repository
- destruction of the folder and associated records.

B5.65 The RKS must alert the Records Manager to disposal policies as they come into force, and seek confirmation before implementing disposal actions; and on confirmation must be capable of initiating the disposal actions.

B5.66 The RKS must enable the allocation of a review decision to a folder or part, or a group of folders, which is undergoing review, including:

- Extension of review period
- re-allocation of a further disposal policy
- selection for export
- immediate destruction following completion of review.

B5.67 The RKS must support the disposal of any paper records associated with the electronic folder that has been authorised for destruction. The support required includes notifying the Records Manager of the existence and location of the paper cover containing the paper records, and recording the confirmation of the destruction.

B5.68 The RKS must destroy the records that have been authorised for destruction.

B5.69 The RKS must remove all references to a destroyed record including knowledge about the record from the Discovery module. All references to the destroyed record will be maintained in the audit log.

B5.70 The RKS must record all disposal actions (review and export) in the folder's Management History and in the audit log, recording:

- The current date and time
- The titles and identifiers of the records actioned
- The disposal schedule applicable
- The identity of the officer who initiated the disposal function (if not automatically initiated)

B5.71 The RKS must record all disposal actions (destruction) in the audit log, recording:

- The current date and time
- The titles and identifiers of the records actioned
- The disposal schedule applicable
- The identity of the officer who initiated the disposal function (if not automatically initiated)

5.1.7.2 Desirable requirements

B5.72 The RKS should enable the reviewer to complete an entry in the management history of the folder or groups of folders being reviewed, as a free-text comment on the review process.

B5.73 The RKS should provide, or support the ability to interface with, workflow facilities to support the scheduling, review and export process, by tracking:

- progress of the review – awaiting, in progress, reviewer details and date
- awaiting disposal as a result of a review decision
- progress of the export process.

B5.74 The RKS should enable the total destruction of groups of folders and individual folders that are stored on re-writable media, by completely obliterating them so that they cannot be restored by use of specialist data recovery facilities.

B5.75 The RKS should provide a facility to define sets of processing rules, which can be applied in a checking and alerting facility to specified folders and groups of folders, prior to initiation of a disposal process.

5.1.8 Workflow for records management

The RKS must support workflow to manage the tasks associated with record keeping. Workflow is used to manage the complete lifecycle of a record, and all actions associated with that record (including all management actions).

5.1.8.1 Mandatory requirements

B5.76 The RKS must be able to electronically notify an action officer of a new record for review/action (this notification must be linked to the corporate electronic mail system).

B5.77 The RKS must be able to track specified time periods associated with various functions and report on these.

B5.78 The RKS must be able to manage all events which have specific triggers associated with them.

5.1.9 Records Manager In-Tray

Records Management staff currently perform some of the classification work for physical records and their assistance will still be required for processing records. An 'in-tray' of tasks to be completed needs to be established with links via the E-mail system.

The functions likely to be passed to an 'in-tray' are:

- Bulk correction of records rejected by the encapsulation or registration process. This may occur because of insufficient or incorrect information provided with the VEO.
- Actions that need to be performed by the Records Manager as a result of event triggers, workflow, requests from users, etc.
- Batch processing of records e.g. re-classification, adjust security, records unavailable, return files to storage (put away) for paper records.

5.1.9.1 Mandatory requirements

B5.79 The RKS must prioritise actions to be performed according to a predetermined priority list. The actions should also have expiry periods associated with them.

B5.80 The RKS must alert the nominated Records Manager(s) by e-mail when a new action item gets added to the in-tray. The e-mail should have a standard subject line in accordance with the priority list and prompt the Records Manager when the item has become overdue.

5.1.9.2 Desirable requirements

B5.81 The RKS should allow separate in-trays for selected users or groups of users (e.g. the InfraRecords Unit of the Department).

5.2 Paper Records Management

The paper record will not be completely replaced by the electronic record in the foreseeable future. DOI will continue creating and acquiring records in paper form, and must integrate management of folders that contain both paper and electronic records.

The model of paper records management is as follows. The folder is always electronic. Paper records are contained within a paper cover (equivalent to a traditional paper folder or file) which is permanently linked to the electronic folder. Management functions are always performed via the electronic folder. Each paper record will have a matching electronic record. This record will contain the descriptive information associated with the record, but will not contain the content of the record.

To manage the paper records that may be registered into the RKS, the following additional functionality is required, and is also shown in a diagram in **Part A – Annexure G – Figure 11 : Paper Records Management Functions.**

5.2.1 General Functions

The RKS must be able to capture, and classify to one or more electronic folders, metadata for paper records and other records arising from the course of business.

5.2.1.1 Mandatory requirements

B5.82 The RKS must be able to register paper records as records – that is, create a metadata profile of a record where the content of the document is not physically held within the RKS.

B5.83 The RKS must support the ability to define different paper record types, with different metadata element sets for each type. Examples of paper record types are:

- correspondence
- maps
- reports.

B5.84 The RKS must be able to associate a paper record with one or more electronic folders.

B5.85 The RKS must be able to retrieve and display the information about a paper record when the electronic folder with which it is associated is retrieved.

B5.86 The RKS must ensure that retrieval of a complete electronic folder also allows the user to retrieve the paper cover (containing the paper records) associated with the folder.

5.2.2 Barcode Functions

The RKS must support barcode labelling of paper records and paper covers, and boxes.

5.2.2.1 Mandatory requirements

B5.87 The RKS must allocate bar codes to paper covers and records, and boxes. The bar codes will be printed out and attached to paper covers and paper records and boxes.

B5.88 The RKS must have the ability to enter data using scanned input instead of keyed data, for example the recording of the movements of paper covers.

5.2.3 Tracking Functions

The RKS must store current (and historical) location management information, have the facilities for paper cover and paper record tracking, and have the ability to perform regular census processes.

5.2.3.1 Mandatory requirements

B5.89 The RKS must store location information, including the ability to set up and maintain office and storage locations in the system.

B5.90 The RKS must record the physical location of paper covers.

B5.91 The RKS must track the movement of paper covers.

B5.92 The RKS must provide the ability to record a specific user or location to which a physical paper cover is checked-out, and to display this information if another user retrieves the folder in the RKS.

B5.93 The RKS must keep an audit trail of the movements of all paper covers.

B5.94 The RKS must support the batch update of system record locations.

B5.95 The RKS must support a paper covers metadata element set which enables the tracking of the physical paper covers associated with a folder, including elements for:

- physical location
- barcode
- check-out to a user
- check-in from a user
- bring forward date.

B5.96 The RKS must support multiple REGISTRY home locations.

B5.97 The RKS should be capable of offering a bring forward facility for paper records profiled in the RKS. This must allow a user to enter a ‘bring forward’ or ‘reserve date’ for a paper record, and generates a subsequent

message for transmission to the current holder of that folder or the Records Manager (according to configuration).

5.2.4 Archival Functions

The RKS must provide for secondary storage and archive procedures of paper covers and the records they contain.

5.2.4.1 Mandatory requirements

B5.98 The RKS must allow the selection of paper covers for archiving (whether they are designated permanent or temporary).

B5.99 The RKS must allocate paper covers to boxes (singularly or in bulk).

B5.100 The RKS must manage the boxes and their storage.

B5.101 The RKS must record metadata about the boxes.

B5.102 The RKS must track box location.

B5.103 The RKS must keep an audit trail of changes/movements of box locations.

B5.104 The RKS must allow the sentencing of boxes. Sentencing a box will automatically sentence the RKS folders of the paper covers contained within the box. As folders contain electronic and paper records, a consequence of sentencing a box will be that any electronic records on the sentenced folders will also be sentenced. Refer to the diagram showing the relationship between a paper cover and the RKS folder in **Part A – Annexure G – Figure 12: Folders and Paper Records**

B5.105 The RKS must be able to export paper record metadata to other VERS repositories.

B5.106 The RKS must be able to use the barcode on the boxes provider by the Department's secondary storage service provider.

5.2.4.2 Desirable requirements

B5.107 The RKS must be able to import paper record metadata from other Agencies.

6. Discovery

6.1 Overview

Through the process of record identification, capture, encapsulation and registration into a record keeping system, the department will build up a significant store of electronic records. The records will be used to satisfy business, legislative and legal requirements of the department, across departments (if the records are exported) and within Public Record Office Victoria. Whilst retaining and managing the records over long periods is a required function of the record keeping system, being able to discover and use records that pertain to a business query is fundamental.

There are two diagrams which illustrate the functions and processes with regard to discovery, **Part A – Annexure G – Figure 13 : Discovery Functions** and **Part A – Annexure G – Figure 14 : Discovery Process.**

Discovery of records can be thought of in two basic ways, browsing and searching. Browsing refers to the method of finding a record by starting at a known point, for example a classification term and following terms linked to this, for example PROJECTS to HERITAGE to HERITAGE ONLINE to PROJECT PLANS. By successively following linked terms (in the form of hypertext links) the user is led to a folder containing records pertaining to the particular project or sub project required. Browsing the web follows this method, i.e. starting at a site and then following subject categories/classifications to the detailed information required. Finding an electronic object on the disk system by using the disk directory structure is another example. Often this method is used when the user does not have an explicit understanding of the information available or location and wants to 'browse' the information base.

Browsing within the context of the RKS needs to be able to commence by user request on:

- any node of the classification structure(s)
- any folder
- any record
- any document
- any linkage between document, folders and other objects
- any term within management control structures

Users will be able to drill up or down from the entry position i.e. from department to finer classification terms, folders, records and documents within the record or alternatively from a particular document up to its containing record, folder and classification.

Users must be able to drill between folders and records by following relations and links, or by utilising implicit knowledge of the RKS (e.g. go to the next record in a folder).

In addition to browsing, users must be able to perform an integrated search for information across the classification structure, records and folders. Users must be able to search the full text of the record/folder content, the content of the metadata elements or both. The user must be able to sort and filter the result set. It should also be possible to perform a subsequent search on the result set to further refine the target information.

To limit the number of departmental information repositories that the user needs to search it is desirable that the RKS indexes can be incorporated into the departmental wide search function provided on the web.

When a search is performed the result set will only contain objects (records, folders and terms) to which the user has access. The access rights that are used by the discovery module must be sourced from the central RKS management user identification control structures or site wide control structures

Through either a browsing or searching process the user will identify the object of interest. The discovery module must be able to display the classification structure, folder and record contents. In addition, if the user requests, it must test the authenticity of the record using the Digital Signature and log any failures. If the user wishes to use a document within a record as the basis for further work then they can select an encoding and save a copy.

Access to a record is defined as the display of the record metadata and/or contents of the record. Details of access to a record will need to be recorded in the audit log and the management history of the record. The listing of a link or a reference to a record in a search result or report is not considered to be an access of the record.

As well as working in an interactive fashion, both the browse and search function must provide an application programming interface (API) that can be incorporated into an application. This will allow the interrogation of the RKS under program control and allow integration with workflow based applications.

Logging of user search requests, access violations and authentication failures is also required.

The Discovery functionality will be delivered by the Web using browsers as the user interface. The design of this Web interface will be based around familiar web concepts. Objects are to be linked together using hypertext links and ‘clicking’ on a link will take the user to the linked object. Information is to be presented as ‘formatted pages’, not ‘screens’.

6.2 Web Access

All online user requests to the RKS discovery system will be by the Web, through Web browsers on the user's desktop.

The following description specifies the functionality required. The design of the actual user interface that implements this functionality is the responsibility of the tenderer and it may have a considerably different appearance to that described here. It is the tenderer's responsibility to develop an intuitive and easy to use interface. As Web designs evolve, it is expected that the functions within the Record Keeping System will make it easy to change the 'look and feel' of the user interface.

Web access will be supported for users in the intranet, internet and extranet domains. User authentication and access control levels will be used to ensure that users can only access appropriate records.

6.2.1 Search Record Keeping System

This function searches the Record Keeping System for folders/records that match a specified criteria and returns a search result set sorted according to a specification.

The search function will support access control on the information it returns. If the user has not supplied a user name and password, a search will only find open access folders and records. If the user has identified themselves, a search will also return folders and records appropriate to that user's permissions.

The search function must support boolean queries composed of tests on:

- the content of a record (if the record has searchable content)
- the content of any metadata element
- the content of a specified metadata element.

The result set must be collapsed (duplicate information suppressed) according to user specified preferences.

Where multiple references to an object are not collapsed they are to be grouped together.

The result set must be sorted according to the user specified preferences.

It must be possible to specify default sorting and display for different objects (folders, records) and for different records and document types. These defaults will be overridden by user settings, if present.

If the information displayed to the user includes a hypertext link, the user will be able to 'click' on the hypertext link to display the record.

The information returned about the records or folders found in a search counts as a minor access to the record or folder. It is desirable that the system records this access. If they are recorded, such accesses should be distinguished from displaying objects or the content.

6.2.2 Display Object

This function displays information (metadata) about a particular object as a Web page. The object may be a classification term, a folder, or a record.

The user will request information by requesting the Web page. The URL of the page should be static so that the users can 'bookmark' the URL in their browser and subsequently retrieve the same page by using the URL.

The contents of the Web page will be dynamically generated from the data held by the Discovery system at the time of the request. If the information includes a reference to another object (classification term, folder, or record), the reference will be a hypertext link. Clicking on the link will display the linked object.

6.2.2.1 Classification Terms

If the object represents a record classification term, the contents of the Web page will include a sorted list of subsidiary classification terms or folders.

The root of the classification tree is to be available at a well known address (URL). This allows external search engines to use Internet searching algorithms ('web spiders') to retrieve all Folders and Records for external searching in a corporate search engine.

6.2.2.2 Folders and Folder Parts

If the object represents a folder, or folder part, the contents of the Web page will include:

- Links to the classification terms in which this folder is located
- The current descriptive VERS metadata about the Folder. Note that the metadata may have been modified since the creation of the Folder.
- Disposal information (if the contents have been destroyed or exported)
- Any links to related folders (sorted by link type). Only folders that the user is permitted to know exist are displayed
- Links to all Folder Parts contained within the Folder
- Links to all records contained within the folder. Only records that the user is permitted to know exist are displayed
- A link to the audit log for the folder. The audit log may be presented as a separate management history log (e.g. metadata modifications, access control policy modifications), usage logs, and preservation logs. Not all users will be able to view all entries in the audit log.

6.2.2.3 Records

If the object represents a record, the contents of the Web page will include:

- Links to the folders in which the record is located
- The current descriptive VERS metadata about the Record as a whole. Note that the metadata may have been modified since the creation of the Record.

- Any links to related records (sorted by link type). Only records that the user is permitted to know exist are displayed.
- A list of the documents contained within the Record. Each document will display the descriptive metadata associated with the document, and a set of buttons, one for each format (encoding) in which the document is represented. 'Clicking' on the button will allow the user to download or display the content.
- A link to the audit log for the record. The audit log may be presented as a separate management history log (e.g. metadata modifications, access control policy modifications), usage logs, and preservation logs. Not all users will be able to view all entries in the audit log.

In the case of 'onion' records the outermost layer of record metadata will be displayed along with the content of the original record which forms the document of the 'onion' record. An option to display the interior layers of metadata will be present.

6.2.2.4 Access Control

The discovery function will support access control on the retrieval of the Web pages containing information on Folders and Records, and on the retrieval of Record content.

6.2.2.5 Usage History

Viewing the metadata associated with a record or folder counts as a minor access to the record. It is desirable that the system records this access. If such accesses are recorded, they should be distinguished from other types of access.

Viewing the content of a record must be recorded.

A usage record must include:

- The date and time of the access
- The type of access (view content, view metadata)
- The user's identity
- The network address and machine name of the computer to which the information was sent.

6.2.2.6 Link to Edit Metadata Function

Having displayed the metadata associated with a Folder or record, it will be possible to edit the metadata of the Folder or record, (Section 5).

6.2.3 Recover Documents

It must be possible to recover documents in their original format from the RKS when they are required. This may be because changes are to be made to the document, or because the document is to be used as the basis for a new record, e.g. cut and paste. The source document in either the long-term form or original format is recovered **but** the original VEO is not changed in any way. If the document is being altered, then a new VEO will be created when it is registered back into the system.

6.3 Requirements for Discovery

The RKS must support Web based searching, browsing and graphical navigation of the classification structure, and the selection, retrieval and display of folders and their contents (records) through this mechanism.

The RKS must support a discovery and delivery API to allow applications to directly interface to the RKS.

The RKS must support access control to prevent returning records or folders to unauthorised users.

6.3.1 Discovery Web Interface

6.3.1.1 Mandatory requirements

B6.1 The RKS must support Web based delivery of the information held by it, including the classification structure, folders, folder parts, and records.

B6.2 The RKS discovery system must implement access control on the Web interface. Users must only be able to access folders and records they are authorised to access. If the user does not supply a user name/password, the discovery system must only return open access folders and records.

B6.3 The RKS must provide a simple search screen that provides minimal options to the user. A minimal search screen could be similar to a Web search engine, providing the ability to do a full text search over the metadata and content. A small number of search options may be provided (e.g. restrict the search to common metadata elements such as title, subject). Predefined sorting and display options will be applied to the search results.

B6.4 The RKS must provide a Web search screen. The user will be able to search

- the content of the record (if the record has searchable content)
- the content of any metadata element
- the content of a specified metadata element.

The user must be able to specify a boolean query with tests appropriate to the data type:

- Strings: equality, contains, lexicographic ordering (before, after), and regular expressions
- Numeric: equality and ordering (<, <=, >, >=)
- Booleans: equality
- Dates: equality and ordering (before, after).

The result set must be collapsed (duplicate information suppressed) according to user specified preferences. These can be expressed:

- Collapse multiple references to the same record to one reference (with, at the user's option, a reference to the original number of references)
- Collapse multiple references to the same folder to one reference (with, at the user's option, a reference to the original number of references)

- Collapse multiple references to the same classification term to one reference (with, at the user's option, a reference to the original number of references)
- Collapse multiple references to the same agency to one reference (with, at the user's option, a reference to the original number of references).

Where multiple references to an object are not collapsed they are to be grouped together, if they are sorted equally.

The user must be able to specify that the result set is to be sorted according to a specified criteria (relevance, or by particular metadata elements). The user must be able to specify that duplicates in the result set can be suppressed.

The result set must be sorted according to the user specified preferences. These preferences will be expressed as:

- Relevance ranking of record
- A list of metadata elements. The first metadata element is to be used as the first sort key, the second as the second key, and so on. The user will be able to specify, for each metadata element whether the list is to be sorted in increasing or decreasing order.

The user must be able to control the information displayed. The user can specify:

- Which metadata elements are to be displayed from the set of metadata elements relevant to that record
- The order in which they are to be displayed
- How much of the contents of each element is to be displayed
- Whether a hypertext link to the record is to be included (default is to include a hypertext link).

Each reference to a found object must be a hypertext link that allows the user to retrieve a Web page describing that object.

B6.5 It must be possible to specify default sorting and display for different objects (folders, records) and for different records and document types. These defaults will be overridden by user settings, if present.

B6.6 If the information displayed to the user includes a hypertext link, the user will be able to 'click' on the hypertext link to display the record (see next function).

B6.7 The RKS must provide the ability to display the classification structure(s) as a Web page or pages. The root of the folder classification tree is to be available at a well known address. The URL of each page must be static (so that users can bookmark a classification structure page and subsequently retrieve it again). The content of each page must be dynamic (i.e. the content is regenerated upon each retrieval so as to be up to date).

The information displayed about each classification term must include: hypertext links to its superior, subordinate and related terms; hypertext links to folders included within the term; and descriptive information about the term.

The RKS must support an 'edit term' button on each classification structure page. This provides a link to invoke an 'edit metadata' function that allows authorised users to edit the classification structure.

B6.8 The RKS must provide the ability to display information (metadata) about a folder or folder part as a Web page. The URL of each folder or folder part must be static (so that a user can bookmark a folder or folder part and subsequently retrieve it again). The content of each folder or folder part must be dynamic (i.e. the content is regenerated upon each retrieval so as to be up to date).

The information displayed about a folder or folder part must include:

- a hypertext link to the classification term that contains the folder, or folder that contains this folder part
- hypertext link to the contained folder parts (if any)
- descriptive metadata about the folder or folder part
- disposal information
- hypertext links to related folders (sorted by link type)
- hypertext links to the records contained in the folder.

Authorised users will be able to view the audit log of the folder. The audit log may be presented as a separate management history log (e.g. metadata modifications, access control policy modifications), usage logs, and preservation logs.

The RKS must support an 'edit button' on each page to allow authorised users to edit the folder metadata.

B6.9 The RKS must provide the ability to display information (metadata) about a record as a Web page. The URL of each record must be static (so that a user can bookmark a record and subsequently retrieve it again). The content of each record must be dynamic (i.e. the content is regenerated upon each retrieval so as to be up to date).

The information displayed about a record must include:

- hypertext links to its containing folder(s)
- descriptive metadata about the record as a whole
- hypertext links to related records (sorted by link type)
- the list of documents contained in the record.

Each document in the record will display the descriptive metadata about the document and a set of buttons, one for each encoding of the document. Clicking on the button will download the content. If the record has multiple layers of metadata (i.e. is an onion VEO) only the outer layer of metadata will be displayed, but the user may request the inner layers to be displayed.

Authorised users will be able to view the audit log of the record. The audit log may be presented as a separate management history log (e.g. metadata modifications, access control policy modifications), usage logs, and preservation logs.

The RKS must support an 'edit' button on each page to allow authorised users to edit the record metadata.

B6.10 It must be possible to recover documents in their original format from the RKS when they are required. This may be because changes are to be made to the document, or because the document is to be used as the basis for a new record, e.g. cut and paste. The source document in either the long-term form or original format is recovered **but** the original VEO is not changed in any way. If the document is being altered, then a new VEO will be created when it is registered back into the system.

B6.11 The RKS must provide a function to extract a single or multiple documents from a record. The function must allow the recovery of identified encodings, executing any necessary translation of the encoding back to its original format and then allow the user to either:

- Save to a disk file or files or
- Launch the appropriate application and read in the document(s).

B6.12 The RKS must allow the user to perform record management functions on the records or folders. The RKS must be able to search for and retrieve both electronic and paper records in an integrated manner.

B6.13 The RKS must allow users the ability to request the verification of the digital signatures associated with the records.

B6.14 The RKS must provide the ability to easily create a default display mapping template for any record type or document type. This template will be used by the discovery system to display the appropriate label and metadata for the record or document concerned.

B6.15 The viewing of the content of a record must be recorded in the audit log. The information must include:

- The date and time of the access
- The type of access (view content, view metadata)
- The user's identity
- The network address and machine name of the computer to which the information was sent.

B6.16 The viewing of a record should enable the user to view the documents within the record to be viewed as they were originally created.

B6.17 The RKS must enable a user to print any documents, which can normally be printed, within a record.

6.3.1.2 Desirable Requirements

B6.18 The RKS should interact with the DOI web accessible search engine(s). The DOI search engine(s) must be able to spider over all information on open access within DOI.

B6.19 The RKS should allow it to be easy to change the 'look and feel' of the dynamically generated Web pages. For example: change the colour scheme, add standard decoration (graphics and text), rearrange the presentation of information on the generated pages; add or remove information from the generated pages.

B6.20 The RKS should be configurable to use secure transmission of information over the Web (e.g. encryption).

B6.21 The RKS should allow users to define, store, and use standard search queries.

B6.22 The RKS should provide user assistance by query formulation, including the use of a controlled vocabulary system and thesauri associated with metadata elements.

B6.23 The RKS should support the sorting, printing and saving of search results in variable display formats.

B6.24 The information returned about the records or folders found in a search counts as a minor access to the record or folder. It is desirable that the system records this access. If they are recorded, such accesses should be distinguished from displaying objects or the content.

B6.25 Viewing the metadata associated with a record or folder counts as a minor access to the record. It is desirable that the system records this access. If such accesses are recorded, they should be distinguished from other types of access.

6.3.2 Discovery and delivery API

6.3.2.1 Mandatory Requirements

B6.26 The RKS must implement an API that allows applications to search for and retrieve folders and records.

B6.27 The RKS discovery system must implement access control on the API. Users and systems must only be able to access folders and records they are authorised to access. If the user/system does not supply a user name/password, the discovery system must only return open access folders and records.

B6.28 The RKS Discovery API must provide the same functionality as that provided by the Discovery (Web) interface to a Web user. The calling system must be able to identify and extract information from the information returned by the API.

B6.29 The Discovery API must be documented. The documentation is to include, at a minimum, an orientation overview that describes the API; detailed functional specifications; and annotated examples of use of the API.

7. Reporting

The RKS must provide a variety of reporting tools for the production of statistical and descriptive reports. The Records Manager and Business Unit Managers will use these reports to manage and audit the RKS. There is a need for a set of standard reports as well as the need for user defined ad hoc reports. These reports need to be produced for a nominated Organisation (or Agency), or for all records in the RKS.

Access to a record is defined as the display of the record metadata and/or contents of the record. Details of access to a record will need to be recorded in the audit log and the management history of the record. The listing of a link or reference to a record in a search result or report is not considered to be an access of the record.

7.1 Reporting Tools

7.1.1 Requirements

7.1.1.1 Mandatory requirements

B7.1 The RKS must provide reporting tools for the provision of statistics to the Records Manager on aspects of activity within the classification structure, including:

- folders created, modified, exported, deleted within a given period
- folder parts opened and closed within a given period
- records added to folders within a given period, stratified by user.

B7.2 The RKS must provide reporting tools for the provision of statistics to the Records Manager on aspects of records in the RKS, including

- the number, location of records, and the physical storage space used, by application type and application package version
- the number, location of records, and the physical storage space used, by user
- the number of electronic records versus paper records in a particular folder, etc.
- the number, location of records, and the physical storage space used, by organisation (or Agency)
- the number, location of records, and the physical storage space used, for a particular level in the classification hierarchy.

B7.3 The RKS must provide reporting and analysis tools for the management of retention and disposal policies by the Records Manager, including the ability to:

- notify all disposal policies which will come into force in a given period of time, and provide quantitative reports on folder size and record types, including box information
- compile statistics of review decisions in a given period
- identify, compare and review disposal policies across the electronic classification structure
- identify formal contradictions in retention and disposition across the classification structure
- identify formal contradictions in retention and disposition between the electronic and paper records

B7.4 The reporting tools must comply with the access control and security of the RKS. Users must only be able to access folders and records they are authorised to access. Reports must only include folders and records that the user running the report has access to.

B7.5 The reporting of the content of a record must be recorded in the usage history. The information must include:

- The date and time of the access
- The type of access (report of content, report of metadata)
- The user's identity

B7.6 The RKS must provide the ability to send a report to file, to print and to display on screen.

B7.7 The RKS must be capable of generating the following statistical reports:

- Number of folders created
- Number of folders modified
- Number of folders retrieved and viewed
- Number of folders with modified metadata
- Number of folders deleted
- Number of folders exported (to other external agencies, to PROV, between divisions, business units, agencies within the RKS)
- Number of parts opened
- Number of parts closed
- Number of records added to a folder
- Number of records exported from one folder to another folder

Each report can be defined by a variety of parameters:

- time period
- by division or business unit
- by individuals or group of individuals
- by location

- classification structure
- records containing documents created by an application type, for example, word processing
- records containing documents created using a particular application package version, for example, Lotus Notes R5
- folder identifier range
- record identifier range
- disposal schedule

B7.8 The RKS must be capable of generating the following descriptive reports on folders and records

- Folder lists
- Content lists – records within a folder, documents within records
- Identify folders never retrieved
- Identify records never retrieved
- Records overdue/action required not completed

The reports may be based on any combination of parameters, as listed in the previous requirement, sorted by any metadata field, e.g. list of folders created during January in folder identifier order.

B7.9 The RKS must provide the ability for users to design and use ad hoc user defined reports. The ad hoc reports can be based on any parameter and be sorted by any metadata. Any type of user may define and use an ad hoc report. The RKS will be able to store the definitions of these ad hoc reports for subsequent reuse.

B7.10 The RKS must be capable of generating the following disposition reports:

- Number of folders eligible for disposal
- Number of disposal decisions completed/changed
- Number of contradictions between decisions and policies
- Identify folders eligible for disposal
- Descriptive reports on disposal actions taken in contradiction to the disposal schedule
- List disposal policies
- List of all folders and parts to which a specified disposal policy is allocated
- List the disposal policies applied to all folders and parts below a specified point in the hierarchy of the classification structure.
- List of all folders and parts, which do not have a disposal policy allocated.

Each report can be defined by a variety of parameters:

- by time period
- length of time since a record has been accessed
- by division or business unit
- by an individual or group of individuals

- by classification structure
- application type
- application package version
- disposal policy.

B7.11 The RKS must be capable of generating the following reports from the audit logs:

- All activities (i.e. normal access - read only, modification, exports)
- Security breaches only, such as attempted access by unauthorised users
- Audit trail of specific users
- Audit trail of specific functions
- Failures to export records successfully
- Identification of folders eligible for disposal that have outstanding action on records within the folder.

B7.12 The RKS must be capable of generating the following reports on the structure of information held:

- Descriptive report on classification used on folders
- Descriptive report on classification not used on folders
- List classification structure.

B7.13 The RKS must be capable of generating the following management reports

- List users (internal and external)
- List organisation structure including divisions, business units, and action officers
- List thesaurus
- Identify Thesaurus terms used/not used
- List Access Control Policies
- List of records and folders that need their access reviewed.

B7.14 The RKS must be capable of producing reports on

- Metadata elements used
- Folder types
- Record types
- Document types
- Encoding types.

B7.15 RKS report presentation must include headings, footers and borders, which can be configured by the Records Manager or other authorised staff.

B7.16 The RKS reporting tool must be able to sort by any metadata field, when presenting the report.

B7.17 The RKS must support third party reporting tools.

7.1.1.2 Desirable requirements

B7.18 The RKS should allow the user the option of saving any reports as a record in the RKS. Such reports must be encapsulated into VEOs as per standard record capture processes.

B7.19 Any records listed in a report, should contain a hypertext link to that record.

B7.20 The listing of a record or folder in a report counts as a minor access to the record or folder. It is desirable that the system records this access. If they are recorded, such accesses should be distinguished from displaying the content of the record or folder.

B7.21 The RKS should have the ability for users to schedule reports to be produced automatically. Users should be able to specify

- the frequency that the report is to be run, e.g. daily, weekly, monthly
- the time that the report is to be run, e.g. midnight, end of month
- whether the report is to be produced on a regular ongoing basis or just for a specified time period
- specify parameters relevant to the information to be reported
- specify the location and format of the output.

The Records Manager, or other authorised staff, must have the ability to change or cancel reports scheduled by users.

8. Authentication (Digital Signatures)

For the RKS, authentication has two aspects. The first is the management of the public/private keypairs (and resulting certificates) used to sign VEOs as they are created, transmitted over the network, and exported. The second is the verification of the signed VEOs. The diagram in **Part A – Annexure G – Figure 15 : Authentication & Digital Signature Management Functions & Process** illustrates the concepts discussed in the section.

8.1 Authentication and Audit

It is necessary to store digitally signed VEOs through time and across platforms. A digital signature will need to be verified prior to entering the VEO into the RKS. It will not be necessary to routinely verify digitally signed VEOs once they are captured, as they will be managed within the system in a manner that ensures authenticity. However, it must be possible to audit the digital signatures of a random sample of VEOs. All verifications of digital signatures must be recorded.

The VERS RKS must be capable of storing details of the successful verification of a digitally signed VEOs as part of the management history of the record.

8.1.1 Digital signatures

8.1.1.1 Mandatory requirements

B8.1 The RKS must be able to retain the information that an electronic signature has been verified as authentic in the management history of that VEO. As part of this metadata, the RKS must record details about the process of verification for a digital signature, including the Certification Authority with which the signature has been validated.

B8.2 All verifications of digital signatures must be included within the audit trail and must include the following information:

- the fact that the validity of the signature was checked
- the fact that the validity of the associated certificates was checked
- the date and time that the check occurred.

B8.3 The RKS must be capable of checking the validity of a digital signature at the time of record capture.

B8.4 The RKS must be capable of checking the validity of a digital signature after a record has been captured.

B8.5 The RKS must be capable of auditing the digital signatures. This involves selecting a random collection of VEOs, verifying all the signatures within the VEO; and bringing any signature failures to the attention of the Records Manager.

B8.6 In addition to verifying the accuracy of a public key by checking the certificate chain, the RKS must be able to check the validity of a public key by comparing it to the public key stored in other VEOs signed by the same signer at the same time.

8.1.1.2 Desirable requirements

B8.7 Where an electronic record has been transmitted in encrypted form by a software application which interfaces with the RKS, the RKS should be able to keep as metadata with that record:

- the fact of encrypted transmission
- the type of algorithm
- the level of encryption used.

8.2 Public/Private Keypair Management

The use of digital signatures to authenticate digital records, and (optionally) encryption to provide secure transmission requires the VERS RKS to manage public/private keypairs, and related certificates.

These public/private keypairs will be used by

- the capture components to sign VEOs as they are created
- (optionally) as the basis for encrypting web pages during transmission
- (optionally) as the basis for encrypting VEOs during transmission for export/import.

We expect that public/private keypairs (and the related certificates) will eventually be generated by a Whole of Government Public Key Infrastructure externally to the VERS RKS. It must, consequently, be possible to enter these externally generated keypairs and certificates into the VERS RKS.

However, it is unlikely that a such an Public Key Infrastructure will be in place in the immediate future. Consequently, it is necessary for the VERS RKS to be capable of generating any necessary public/private keypairs and associated certificates. It must be possible to migrate from internal generation to the use of externally generated keypairs.

8.2.1. Certificate Records

In a normal digital signature application, the validity of a public key is checked using a chain of certificates obtained from a Public Key Infrastructure. When checking a digital signature applied to a record, it may be necessary to check certificates that may be decades old. Currently it is felt that a normal Public Key Infrastructure is unlikely to reliably preserve certificates for this length of time. Instead, the VERS RKS will hold any necessary certificates as records (known as 'Certificate Records'). The VERS RKS must be capable of accepting these certificates and generating the necessary certificate records.

8.2.2 Signature Management

8.2.2.1 Mandatory Requirements

B8.8 The RKS must generate public/private keypairs with a key length of at least 40 bits.

B8.9 The RKS must be capable of generating certificates containing the public keys it uses.

B8.10 The RKS must be capable of accepting externally generated public/private keypairs and certificates instead of generating its own keys.

B8.11 The RKS must provide a mechanism to manage the public/private keypairs used by the system to sign VEOs as they are created. There may be only one keypair used to sign all records within the Department, or there may be different keypairs for different record capture systems.

B8.12 The RKS must support the management of the keys used to encrypt data transmitted during user access to records and during the export and import of records.

B8.13 The RKS must create certificate records containing certificates. These certificate records will be handled as normal records within the RKS (i.e. will be expressed as VEOs and filed in a Folder).

8.2.2.2 Desirable Requirements

B8.14 The RKS should allow different keypairs to be assigned to different capture processes.

B8.15 The RKS should provide a mechanism for the creation and management of keypairs for individual users.

B8.16 The RKS must generate public/private keypairs with a key length of at least 128 bits and should have the option to generate longer keys if required.

B8.17 The RKS should be capable of using the existing Lotus Notes infrastructure to encrypt information being transferred (e.g. Web pages to users). This includes the use of the Lotus Notes public/private keypairs.

9. Security & Audit

9.1 Security – Records & Users

Electronic records contain evidence of business transactions and activities and may also contains personal, commercial or other sensitive information. It will be necessary to manage access to these records to ensure compliance with the regulatory environment and corporate policy.

The RKS will need to manage the security and audit of records for each organisation supported by the RKS. This concept is illustrated in **Part A – Annexure G – Figure 16 : Security & Audit Functions.**

Access management aims to strengthen privacy and security while facilitating information sharing. The RKS must restrict inappropriate access, and will be required to support Freedom of Information legislation, Privacy legislation and the goals outlined in the Data Protection Bill. Corporate policy will require that specific records or folders can be protectively marked in order to limit user access to individuals or specified groups; the need to control such access will usually diminish with the passing of time, and will need to be reviewed and revised.

Both corporate policy and the need to retain integrity and authenticity in records will require restriction of access to system functions according to user role.

It will be necessary to ensure that rights of access to records and to functions are granted to authorised individuals and groups, and withheld from unauthorised individuals and groups.

The RKS must support the following functionality:

- Maintain access control policies - this includes the creation, modification, and deletion of access control policies.
- Maintain lists of users and groups of users, as well as roles
- Provide the ability for users to identify themselves
- Apply the access control policies to control access to records and folders held within the RKS
- Apply the access control policies to control access to RKS functions.

This section is structured in the following fashion:

- The first part deals with the management of access control policies.
- The second part deals with the application of these policies to controlling access to records and folders
- The third part deals with the application of these policies to controlling access to RKS functions and facilities.

Note that the following access control model is for explanatory purposes only. A tenderer must implement the functions and capabilities specified in this section, but

may choose to do so using a different method (e.g. by using capability lists instead of access control lists).

9.1.1 Access Control Policy Management

This section deals with the general management of the access control policies.

9.1.1.1 Mandatory requirements

B9.1 The RKS must support access control policies that grant access rights over controlled objects to specified users.

B9.2 The RKS must support and manage access control policies for each organisation (Agency) whose records are managed by the RKS.

B9.3 The RKS must support the following controlled objects:

- RKS functions, particularly management functions
- Folders
- Records.

The possible access rights will vary depending on the type of controlled object.

B9.4 The RKS must support the management of users. User information should, where possible, be sourced from the existing Lotus Notes environment. At minimum, users should have the same user account names in the RKS as in the FOI environment. This function allows the creation, removal, and suspension of users in the RKS, and the modification of information held about the users (including the setting of passwords). Information about a user is to include their name and position within the organisation. Suspension of a user account means to have the account turned off; users cannot use the account, but the account information is not actually deleted.

B9.5 The RKS must allow users to identify themselves when accessing the system (e.g. by password or by account information).

B9.6 The RKS must support the management of groups. This function allows the creation, modification, suspension, and removal of groups of users. Members of a group may be an individual user or other groups. Suspension of a group means to have the group turned off; members of the group cannot use the account, but the group information is not actually deleted. A special, pre-defined group, will be ‘All users’.

B9.7 The RKS must support the management of ‘roles’. A role is associated with permitted functionality within the RKS and differs from a group. The RKS must allow individual users or groups to be allocated a role. Roles and the associated functionality must be able to be created, modified and deleted.

B9.8 The RKS must be able to produce reports linking a decision to grant (or deny) access to an object to the policies that determined this decision; and the policies associated with a particular object or associated with a particular user.

B9.9 The RKS must provide a user interface that allows the creation, modification, and deletion of the access control policies.

B9.10 The RKS must restrict the ability to allocate and amend access control policies on electronic records and electronic folders to:

- the owner of the record or folder in all cases
- the Records Manager
- the Records Manager, where no other user has current access.

9.1.2.2 Desirable requirements

B9.11 The RKS access control management interface should be implemented over the Web.

B9.12 The RKS should support the allocation of access controls that are valid for a specified time period, and should notify the Records Manager prior to the termination of that period.

B9.13 The RKS should allow the Records Manager to *deny* users or groups access to objects. (The access control model given above *grants* access. It is sometimes more convenient to generally grant access and then explicitly deny access to specific users or groups.)

B9.14 The RKS should allow the management of the organisation hierarchy and the positions within the structure.

9.1.2 Control of access to folders and records

This section deals with the application of access control policies to folders and records held within the RKS. Some folders and records within the RKS will contain sensitive information and access to these records and folders needs to be restricted either due to business or legislative requirements. This restriction of access needs to be reviewed after specified time periods according to the type of record or folder.

9.1.2.1 Mandatory requirements

B9.15 The RKS must support the creation and management of access control policies.

B9.16 The RKS must control access to records and folders according to the access control policies in force.

B9.17 The RKS must support access control policies which consist of a review period, a set of instructions regarding the granting of access, the name of the officer to approve access, and the roles, individuals, and groups of users who are permitted access under this policy, and the type of access permitted.

B9.18 The access control policy must define the period when records and folders controlled by a particular policy are reviewed. The review period, which can be expressed as a passage of a period of time, the occurrence of a

specified event (e.g. change of government), the passage of a period of time following a specified event.

B9.19 The RKS must track review periods for records and folders, and initiate the access control policy review. The access control policy review must allow the Records Manager to either confirm or modify the access policy to the records or folders.

B9.20 The access control policy can be applied to all folders within the RKS, to all folders within a particular branch of the classification structure, to a specific folder, or to an individual record.

B9.21 The RKS must allow the modification of an access control policy, and for this change to be reflected throughout the RKS. A record of the change must be documented in the Audit Trail.

B9.22 The RKS must allow the removal of an access control policy, but not all policies.

B9.23 The RKS must be capable of assigning an access control policy to any term in the classification structure, folder, or folder part. The classification structure, folders, and folder parts form a tree, and an access control policy applied to any node in this tree applies to any subordinate node (classification term, folders, and folder parts) unless over-ridden by a policy applied to the subordinate node.

B9.24 The RKS must enable an access control policy to be allocated to a specific folder or record, and this policy overrides the default policy allocated at a higher point in the classification structure.

B9.25 The RKS must support an access control policy where the default access is no access is granted; and users must be explicitly granted access to each object.

B9.26 The controlled objects are folders and records. The RKS must have controls that may apply to:

- An individual record
- Individual metadata elements
- All records within a particular folder
- All parts within a folder
- All records within a particular classification
- All records
- An individual folder
- All folders within a particular classification
- All folders belonging to an organisation (or Agency)
- All folders.

B9.27 The RKS must support the following access rights for folders and records:

- None. No access is allowed

- Know exists. User is able to know that a record or folder exists (e.g. a record will appear in the list of records within a Folder), but cannot retrieve any details about the records or the folder
- View selected metadata. User is able to view selected metadata according to their role. The Records Manager must be able to define selected sets of viewable metadata for each role.
- View metadata. User is able to view the metadata associated with a folder or record, but not retrieve the content.
- Modify metadata. User is able to modify the metadata associated with a Folder or record.
- Retrieve content. User is able to retrieve the content of the record.
- Sentence. User is able to sentence the record for disposal. This implies full access to the content of the record as the user may need access to the record to confirm the sentence.

B9.28 When access control is modified, the RKS must retain the previous control(s), and the date of the amendment, as a part of the management history metadata element for that electronic record or electronic folder.

9.1.2.2 Desirable requirements

B9.29 The RKS should be able to apply policies to records or folders that match an arbitrary combination of metadata.

9.1.3 Control of access to system functions and facilities

This section deals with the application of access control policies to the RKS functions (i.e. allowing users to execute specific RKS commands).

9.1.3.1 Mandatory requirements

B9.30 The RKS must be able to limit access to system functions and facilities, so that all users will only be able to carry out functions that are assigned to the user role(s) of which they are member(s). Note that wherever 'user' appears in this section, a 'group of users' may appear.

B9.31 The RKS must ensure that all users are allocated to one or more user role(s).

B9.32 The RKS must support an access control policy where the default access is that no access is granted; users must be explicitly granted access to each function.

B9.33 The controlled objects are the RKS functions and collections of functions.

B9.34 The RKS must support the following access rights for functions:

- None. No access is allowed
- Execute if owner. The user is able to execute the function if it operates on an object owned by the user. For example, a user might be able to execute the 'modify access control policy' function if the policy being modified was owned by the user

- Execute. The user is able to execute the function.

B9.35 The RKS must be capable of removing the visibility of functions from users who do not have access to those functions in their allocated user role.

9.2 Audit

An audit trail which tracks actions taken on users, records and folders relating to declaration, access, management, preservation and disposal will be necessary to demonstrate authenticity throughout the record lifecycle.

The RKS must keep an unalterable audit trail capable of recording all the actions that are taken upon a record, folder or classification structure; the user initiating the action; and the date and time of the event.

The RKS must be able to maintain audit trails for the life of the record and folder, and be able to export audit trails for users, records and folders.

The RKS must be capable of storing details of the successful verification of a digitally signed record as metadata with the record itself.

The following are examples of audits that will need to be performed:

- Digital signature audit - This function selects records at random and checks the digital signatures for accuracy. All the signatures within a record are checked (including the signatures on the various layers of onion records and the signatures on the certificates included in the signature blocks)
- Completeness audit - This function selects folders at random and checks that the folder exists, and that all records within the folder exist.
- User audit of actions taken
- Record audit of actions taken
- How often have records been used (viewed or edited)
- Last time records accessed (viewed or edited)
- Requests for change to user access rights.

9.2.1 Requirements

9.2.1.1 Mandatory requirements

B9.36 The RKS must keep an unalterable audit trail of events within the system, that records:

- the records management or system management function which is being applied
- the object(s) to which the function is being applied
- the user applying the function
- the date and time of application

where events occur to:

- classification structure
- thesaurus
- controlled vocabularies
- access control policies
- disposal schedules
- folders
- folder parts
- records
- organisation (or Agency).

B9.37 The RKS must allow the extent of audit trail tracking and recording to be user-configurable, so that a Records Manager can select the functions which are automatically recorded; the RKS must then ensure that this selection itself is recorded and that all changes are recorded.

B9.38 The RKS must have the default setting for the audit trail as “on”, with the ability to turn it “off” for particular types of objects.

B9.39 The RKS must track and record events automatically without manual intervention.

B9.40 The RKS must ensure that audit trail data cannot be modified in any way or deleted by any user.

B9.41 The RKS must maintain the audit trail for as long as required, which will be at least for the life of the record or folder to which it refers.

B9.42 The RKS must ensure that audit trail data is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that authorised external personnel can achieve this who have little or no familiarity with the system.

B9.43 The RKS must be able to export audit trails for records and folders and with the option to delete the relevant events from the audit trail.

B9.44 The RKS must be able to record violations, and attempted violations, of access control mechanisms.

B9.45 In particular, the RKS must be capable of recording in the audit trail the following information:

- the date and time of declaration of all records
- the initial, and any subsequent, entries of a record within the RKS structure
- re-location of a record, or a group of records, to another folder
- re-location of a folder, or a group of folders, within the RKS structure
- re-allocation of a disposal schedule to a folder
- the occurrence of a change made to any metadata associated with folders or records
- changes made to the allocation of access control of a folder, record or user
- export actions carried out on a folder
- deletion / destruction actions on a folder or record.

B9.46 The RKS must be capable of registering the destruction of records, folders and groups of folders in an audit trail for *permanent preservation*.

B9.47 The RKS must be capable of recording all possible events in the audit trail.

B9.48 The RKS must be capable of recording the data changes made during any recorded event in the audit trail.

B9.49 The RKS must keep a separate audit trail for each organisation (or Agency).

10. System Management Functions

This section of the specification will cover areas such as, general management commands, maintainability, reliability, media management, status report, emergency recovery, document type definitions (DTD), record retrieval (look and feel), system access control and system parameters, as illustrated in **Part A – Annexure G – Figure 17 : System Management Functions.**

The evaluation of the general management commands will include:

- Startup
- Shutdown - Shutdown modes include both immediate and delayed (where no new functions are accepted, but existing functions are run to completion).
- Resync - Resynchronises any volatile databases (e.g. knowledge of which media are loaded) with reality.

The maintainability evaluation will consider the extent to which the VERS Record Keeping System includes features that allow its Records Manager to maintain it, including:

- The ability to make bulk changes in record organisation and folder structure and to indexing information, and to ensure all metadata and audit trail data are handled correctly, in order to make the following kinds of organisational change[1]:
  - support for multiple organisations (or Agencies) within the RKS
  - division of an organisational unit into two
  - combination of two organisational units into one
  - movement or re-naming of an organisational unit
  - division of a whole organisation into two (or more) organisations.
- The ability to support the fluid movement of users between organisational units, and organisations, individually or in bulk.
- The ability to retrieve, display and re-configure systems parameters and choices made at implementation – for example, on elements to be indexed – and to re-allocate users to user roles, and functions to user roles, in a controlled manner and without undue effort.
- The ability to monitor available storage space, and provide notification to Records Manager when necessary.
- The extent of commitment to ongoing development and support, so that the organisation can be confident of upgrade as a result of developments in systems and application software.
- The ability to specify and manage access control rules.
- The ability to manage the storage media.

[1] Note: In the following, changes to organisational units imply corresponding changes to the classification structure of the units and their user populations.

Reliability evaluation will consider the extent to which the VERS RKS includes features that ensure that the records held by the system are held reliably:

- Evidence of the effort put into ensuring that VEOs are not lost or corrupted once accepted by the system
- The ability to provide back-up facilities and to rebuild forward using back-up and audit trails
- The ability to provide recovery and roll back facilities in the case of system failure or update error, and to notify the Records Manager of the results.

The media management function manages the media contained within the Record Keeping System. Among other activities supported by this function is refreshing of the media on which the records are stored. Refreshing is the copying of the contents of a piece of media to fresh media (possibly using a different storage technology or density). Aspects of this activity includes:

- Determination of when media requires refreshing (based on, for example, the number of times a piece of media has been used, the measured bit error rate, or the age of the media)
- Verification of the media before writing (if required)
- Copying the records from the media and verifying the accuracy of the copy.
- Removal and physical destruction of the original media.

The status report function displays the status of the Record Keeping System. It includes statistics on:

- The number of folders and records stored in the system
- The rate at which the various functions are being executed.
- The amount of storage free/used
- The current (spot) usage (e.g. number of searches, reports, and creation of records).

The emergency recovery functions will cover the ability to recover the contents of the Record Keeping System after a catastrophic failure. The function will recover all internal databases.

The document type definition function modifies the XML Document Type Definition (DTD) that specifies the structure of the VERS records. Modifying the DTD will be used to add additional metadata elements if this is required.

The existing records in the Record Keeping System need not agree with the modified DTD.

The Search Record Keeping System Function must be capable of searching on the new metadata elements of the modified DTD. The Display Record Function must display the new metadata elements of the modified DTD. The modifications to the Web interfaces that provide these functions will be performed automatically from the DTD, although some additional information may need to be provided by system managers (e.g. text for help screens).

Modify record retrieval function modifies the look and feel of the Web pages generated by the Search Record Keeping System and Display Record functions.

The user will be capable of modifying the general style of the Web pages (e.g. background, decorations, standard buttons, frames, character styles).

The user will be capable of modifying the layout of information on the Web pages (e.g. ordering and placement of information on the page).

The system access control functions will controls access to the Record Keeping System Resources. These resources include:

- Functions (execute function)
- Access Control and Sentencing Policies (create, modify, and delete policy)
- System access control (create, modify, and delete)
- Parameters (modify)

The system modify function allows the modification of system parameters, including:

- Web addresses upon which the Record Keeping System is listening for requests and commands
- Maximum number of search/retrieval requests allowed per user at any one time
- Web address blocks (e.g. filters that block Web access to the Record Keeping System unless the user is logged onto a host with an authorised IP address).

10.1 Mandatory Requirements

B10.1 The system management must allow the Records Managers to maintain the information related to organisations (or Agencies) whose records are managed by the RKS.

B10.2 The system management must allow the Records Managers to maintain the classification structures in the Record Keeping system.

B10.3 The system management functionality must allow the Records Managers to maintain the users individually or groups of users within the Record Keeping system.

B10.4 The system management functionality must allow the Records Manager to manage 'Message of the Day' for users accessing the RKS.

B10.5 The system management functionality must allow the Records Manager to identify users actually connected to the system and allow a 'Connected Users' message to be sent to these users. The message must display to the front of the screen and must require acknowledgment by the user.

B10.6 The system management functionality must allow the Records Manager to deny access to all new users and for a suitable message to be displayed to these users.

B10.7 The system management functionality must allow the Records Manager to deny access to new records to already connected users, and for a suitable message to be displayed to these connected users.

B10.8 The system management functionality must allow the Records Manager to disconnect any nominated connected users after the display of a suitable message and the elapsing of the specified number of minutes (which may be set to zero). The system management functionality should cleanly disconnect these users and not leave 'connected sessions' or unsaved data. Any unsaved data will be lost.

B10.9 The RKS must be capable of being immediately shutdown (i.e. all current operations are aborted). The internal RKS data must, however, be left in a consistent state and no records can be lost. This functionality is to be restricted to the IT Systems Manager.

B10.10 The RKS must be capable of being shut down in a delayed mode. In this mode all current operations are completed, but no new operations are accepted. A suitable message must be sent to all users. The internal RKS data must be left in a consistent state. This functionality is to be restricted to the IT Systems Manager.

B10.11 The system management must allow the Records Managers to maintain the access control policies within the Record Keeping system.

B10.12 The system management must allow the Records Managers to maintain the disposal policies set out by Public Record Office Victoria for a specified organisation or a generic disposal schedule.

B10.13 The system management must allow the Records managers to maintain the paper and electronic folder numbering individually or in bulk.

B10.14 The system management must allow for the maintenance of the creation and assignment of digital signatures and the recording and assignment of certificates. This functionality is to be restricted to the IT Systems Manager.

B10.15 The system management must allow the Records Managers to maintain the Thesauri or Thesaurus and one or more controlled vocabulary conventions.

B10.16 The system management must allow the Records Managers to maintain locations and the ability to alter the location of a user or record within the system individually or in a bulk process.

B10.17 The system management must allow the Records Managers to maintain the number of auditing levels as set out in section 9.2.1 of this document.

B10.18 The system management must allow for the maintenance of the emergency recovery processes for all internal databases and contents. This functionality is to be restricted to the IT Systems Manager.

B10.19 The system management must allow for the maintenance of the system parameters including, web addresses, search and retrievals. This functionality is to be restricted to the IT Systems Manager.

B10.20 The RKS must be capable of resynchronising any volatile data with the underlying permanent store. This functionality is to be restricted to the IT Systems Manager.

B10.21 The RKS must be capable of displaying and modifying system parameters and choices made at implementation. In particular, this includes: the address upon which requests and commands are accepted and the maximum number of search/retrieval requests (both in total and per user). This functionality is to be restricted to the IT Systems Manager.

B10.22 The RKS must support Web address blocks (i.e. blocking connection requests unless from an authorised IP address). This functionality is to be restricted to the IT Systems Manager.

B10.23 The RKS must be capable of monitoring available storage space. It must be capable of notifying the Records Manager when available storage falls below a threshold. This threshold must be capable of being set by the IT Systems Manager.

B10.24 The RKS must be capable of monitoring the usage of media usage by Agencies, Divisions, business units, and by individuals or groups of individuals.

B10.25 The RKS must be capable of tracking each piece of media in the system and determining when the piece needs to be refreshed. This may be based on the number of times the media has been used, the measured bit error rate, or the age of the media. The thresholds for this decision will be set by the IT Systems Manager and can be set for different media types and manufacturers.

B10.26 The system management must allow for the maintenance of the media when the media requires refreshing (based on, for example, the number of times a piece of media has been used, the measured bit error rate, or the age of the media). Verification and the removal and destruction of the original media, is a requirement. This functionality is to be restricted to the IT Systems Manager.

B10.27 The RKS must verify each copy of data to or from a piece of media

B10.28 The RKS must allow the removal and physical destruction of a piece of media.

B10.29 The RKS must provide a status report function that displays the ongoing status of the RKS. This report will include: the number of folders and records stored in the RKS, the rate at which various functions are being executed, the amount of storage used/free, and the current (spot) usage.

B10.30 The RKS must provide the ability to recover from a catastrophic failure of any part or parts of the system. The recovery system must bring the internal data back into a consistent state and must not lose any records entrusted to the care of the RKS.

B10.31 The RKS must provide the ability to maintain and modify the VERS XML DTD. It must not be necessary for existing VEOs to be modified to conform to the modified DTD. The Search and Display functions of the Discovery system must be capable of searching and displaying all VEOs within the system, both to the unmodified and modified DTD. The modifications to the Web interfaces that provide these functions will be performed automatically from the modified DTD, although some information may need to be provided by the Records Manager (e.g. help screen text).

B10.32 The RKS must have a spell check facility for all areas of the system.

B10.33 The RKS must have a virus check for documents going into the system.

B10.34 The RKS must have a comprehensive online help facility available to the users.

B10.35 The system management must allow for the maintenance of record types as defined in section 5.1.6 of this document.

B10.36 The system management must allow for the maintenance of workflow processes within the Record Keeping system.

B10.37 The system management must allow for the maintenance of barcoding functions within the Record Keeping system.

B10.38 The system management must allow for the maintenance of the discovery function using either a predefined or a default view.

B10.39 The system management must allow for the maintenance of reporting functions from the Record Keeping system as defined in section 7.1 of this document.

B10.40 Based on current staffing levels, the system will need to be able to support the following:

- Read access for a minimum of 750 users
- Web discovery access for a minimum of 750 staff
- Update access for a minimum of 750 staff
- Records Manager level access to a minimum of 10 staff
- Adhoc reporting capability for a minimum of 750 users
- Concurrent access (any type) by 400 users.

11. Implementation, Training, Documentation and Support Considerations

DOI requires a system that has training and reference manuals of sufficient quality and clarity to enable the departmental staff to effectively configure, support and operate the system.

11.1 Phased Approach

After selection of the preferred system, its modification, testing, and acceptance testing, DOI will implement the RKS in a pilot group composed of two business units. Subject to a satisfactory pilot stage, DOI will then implement the system on a business unit basis. This is to allow business units that share the same set of records to be converted as a group. A business unit may have staff members who are located at different locations throughout Victoria.

11.2 Training Approach

The Department has a training facility at Nauru House that is used to conduct computer-based training courses. The facility can be used to train 10 staff and contains 11 networked PCs built to the common desktop standard CDSE environment. Whiteboards, overhead projector, and Boxlight data projection equipment are also available.

B11.1 Tenderers are requested as part of their response to the RFT to outline their approach to training for system administrators, help desk operators, records managers, action officers, general users and staff members located at regional offices.

11.3 Training Courses

B11.2 Tenderers are requested as part of their response to the RFT to provide details of their training courses including:

- name of course
- topics covered
- expected duration
- intended audience of course
- any prerequisite training and/or knowledge
- training materials provided
- whether the course is offered as a Computer Based Training module
- hardware, software, and other requirements to conduct course on DOI premises at Nauru House.

The following course types are suggested:

- Introductory course – for general users covering discovery and retrieval of records, and the use of standard reporting tools

- User course – for action officers covering creation and management of records and folders
- Advanced course – for Records Managers covering all the system management and configuration features
- Technical course – for the Information Technology staff covering all technical system administration features
- Overview course – for management, helpdesk operators and other staff requiring an understanding of the key features of the system
- Train the Trainer course – to train DOI staff who will be responsible for conducting individual or refresher training courses.

11.4 Documentation

11.4.1 Types of Documentation

11.4.1.1 Mandatory Requirements

B11.3 The following documentation is the minimum expected to be delivered with the RKS:

- Training course manuals (one for each type of course)
- User guides (for general users, for action officers, and for help desk operators)
- Administration guide for records managers
- Report Writer Manual

B11.4 The following documentation is the minimum expected to be delivered as System Administration guides for IT technical staff

- General overview of the system and its operation
- Audit logs
- System monitoring and management procedures
- System backup and recovery procedures
- Security and Audit manual
- Support/ Utility programs manual
- The set up, configuration, and operation of any hardware included as part of the VERS RKS, particularly specialised hardware such as media management
- The set up, configuration, and operation of any supporting software included as part of the VERS RKS (e.g. databases)
- API manuals
- System documentation covering topics such as error messages, routine housekeeping activities
- Any other operational procedures.

11.4.2 Format of Documentation

11.4.2.1 Mandatory Requirements

B11.5 All documentation is to be provided on paper and also in electronic format produced in Microsoft Office 97 products, PDF, or Visio.

11.4.3 Customisation and reproduction of documentation

11.4.3.1 Mandatory Requirements

B11.6 The Department requires the ability to customise all documentation to suit DOI's purposes and the Department's configuration of the software.

B11.7 The Department will own the copyright of any customised documentation, or have the right to reproduce copies of the customised documentation.

B11.8 The Department will own the copyright of any documentation that is specially written for DOI as part of the contract.

11.5 System Support

B11.9 Tenderers are requested, as part of their response to the RFT document, to outline their approach to support.

Support will include the following issues:

- Problem solving with the application and the system environment
- Identifying training needs
- Identifying software and hardware problems and arranging appropriate solutions
- Scheduling implementation of upgrade releases
- Managing performance standards.

B11.10 Tenderers are requested to provide the following details in their response to the RFT:

- Hours of support available
- Guaranteed response time
- Hotline support
- Maintenance services
- Software updates and new releases
- Escalation procedures
- Disaster Recovery situations.

B11.11 System support will need to be provided during

- the development of new modules or extensions to existing modules of the standard package, to meet requirements
- acceptance testing

- implementation.

B11.12 System support will be provided to the project team and to the DOI IT technical staff supporting the development environment.

11.6 Operational Support

B11.13 As it is possible that the system will differ significantly from the systems currently supported by DOI, Tenderers are requested to outline their approach to operational support and the possibility of operating the system after installation.

11.7 Service Level Issues

11.7.1. On-going Development

The VERS RKS will be a complex system with an ongoing requirement for support in the following areas:

- Capture integration with applications. In addition to reintegrating record capture into new versions of applications, there will be ongoing work integrating record capture into new applications.
- Evolution. The VERS RKS is a new system. It is expected that the requirements will evolve as experience is gained in using the system, and this will require modification of the system.
- Integration with other business requirements. The VERS RKS is a new system. It is expected that as knowledge and experience of the system grows within DOI, it will become one of the widely used corporate information repositories and will need to be integrated with other information repositories.

11.7.2 Customer Service Framework

B11.14 It is expected that system support will be provided in accordance with an ongoing support and maintenance agreement, with a Service Level Agreement, for a period of 5 years. In particular, Tenderers should note how they propose to update software (e.g. update to Windows 2001) as this is required by DOI.

B11.15 Tenderers are requested, as part of their response to the RFT document, to outline their Customer Service Framework and their approach to Service Level Agreements and on-going development and support. This is to include formal processes for problem management, delivery of software, upgrades of software, etc.

B11.16 DOI requires the Vendor to provide reports on compliance with Service Level Agreements. Tenderers should state in their response what reports that will provide, and provide examples where possible.

B11.17 Tenderers are requested, as part of their response to the RFT document, to outline their approach to post-implementation consultancy and change management services. Costings for these services should be included in the Tender Sum Information in Part D – Schedule 12.

11.7.3 Performance Standards

11.7.3.1 Mandatory Requirements

B11.18 Performance standards for the system should provide the following response times at a minimum:

- Simple transactions 98% in < 1 second
- Medium transactions 98% in < 5 seconds
- Complex transactions by negotiation.

Issues to include:

- Measurements taken from the end user point rather than internal system measurements
- Classification of transactions
- Performance applicable at Head Office and regional offices.

B11.19 System availability should be:

- Prime time 99%
- Non Prime time 95%.

Prime time is defined as Monday to Friday 8.00am to 6.00pm, except for recognised Victorian-wide Public Holidays.

B11.20 Frequency of backups will include:

- Nightly
- Weekly
- Monthly.

B11.21 Contingency plans will be designed for any outage period longer than 3 hours. Recovery of the system without loss of records will need to be guaranteed. These plans and the testing of these plans will be a key deliverable of the project, and need to be included in the project plan.

12. Technical Requirements & Design Considerations

12.1 Ease of use

The evaluation will consider the extent to which the proposed VERS RKS is easy to use for the following groups of users:

- Users finding and retrieving records
- Users registering records; particularly the ease of use when capturing records from the file system and Lotus Notes
- Records Managers
- IT System Administrators; particularly with regard to the integration of the various components that make up the VERS RKS, and with regard to media management.

Issues:

- The provision of on-line help throughout the VERS RKS, and the extent of any context-sensitive help facility
- The extent to which the user interface is consistent, both internally (i.e. between the various functions of the VERS RKS) and externally (i.e. the use of a standard 'look and feel' with other PC applications)
- The extent to which the VERS RKS is intuitive to users; that is how closely does the user interface match user models of how an RKS works
- The extent to which commonly used features are easy to use and learn
- The ability to move from performing simple operations to performing complex operations without learning a new interface
- Minimising the amount of training required for new users
- The appearance and organisation of information; particularly the design of screens and the arrangement of information on them to maximise the amount of information displayed while minimising confusing clutter
- The extent to which all error message are meaningful, and can be appropriately acted upon, by the users who are likely to see them
- The look and feel of the Web interface used for searching and browsing. This must be easy to use and intuitive throughout
- The suitability of the user interface for users with disabilities; that is, compatibility with specialist software that may be used and with appropriate interface guidelines. Refer to **Human Rights and Equal Opportunity Commission Working Paper on Web Accessibility**
- The ability of users to move, re-size and modify the appearance of display windows, to select sound and volume of audio alerts, and to save modifications in a user profile

- The provision of persistent, user-definable defaults for data entry where desirable.

12.1.1 Mandatory requirements

B12.1 Tenderers are requested to provide details of their user interface design approach as part of their response in Part D – Schedule 4.2 Methodology.

12.2 Capacity

12.2.1 Estimated Capacity Requirements

The following figures should be used to estimate the capacity requirements of the RKS:

Current measurements of usage for information and records:

- Network File System disk space usage is 250GByte with a growth of 10 GByte per month.
- Electronic Mail - up to 800 MByte per day sent & received, or 16 GByte per month. Approximately 40 GByte of electronic mail is stored at any time.
- The existing Records Management Systems currently manages about 200,000 folders and 300,000 documents (most documents are not registered separately). The Recfind system occupies approximately 2 GBytes and the Trim system occupies approximately 3GBytes.

Tenderers should assume each VEO is around 1 Mbyte in size, (this would be an overestimate for records sourced from Word files). Scanned documents are about 2 MByte for 20 pages, giving approximately 100K per page.

Tenderers should assume a growth rate of 25 GBytes per month of VEOs.

Tenderers should allow for an initial capacity of 500 GBytes. It is expected that this capacity will be filled within 1 to 2 years. Tenderers should allow for the intial system to contain 700,000 records and 300,000 folders.

Tenderers should allow for a growth to 5 Terabytes with a tenfold increase in the number of documents and folders over a 5 year period.

12.2.2 Capacity Issues

The evaluation will consider the extent to which the proposed VERS RKS fulfils the following capacity requirements.

- Expected number of records (700,000 records, 300,000 folders);
  maximum number of records (7 million records, 3 million folders);
  ease of expanding beyond maximum capacity
- Expected storage capacity (500 GBytes);
  maximum capacity (5 terabytes);
  ease of expanding beyond maximum capacity
- Expected request rate (10 requests per minute);
  maximum rate (100 requests per minute);
  ease of expanding beyond maximum rate
- Expected submission rate (2,500 records per month);
  maximum rate (5,000 per month);
  ease of expanding beyond maximum rate
- Maximum size of individual records (100 MBytes)
- Speed: Submission (under 5 seconds per record registration),
  Searching (under 1 second),
  Display of record content or metadata (under 1 second),
  Management Functions (typically under 1 second, depending on complexity of function)
- The ability with which the VERS RKS provides adequate response times (as per 11.7.3 Performance Standards) for commonly performed functions under standard conditions, for example:
  - 75% of the total anticipated user population (750 users) logged on and 400 active users
  - 100% of the anticipated total volume of documents managed by the system
  - users performing a mix of transaction types at various rates

  with consistency of performance over at least ten transaction attempts.
- The ability to allow a system implementation to be expanded, in a controlled manner, up at least 4000 users while providing effective continuity of service.
- The ability to support the above without imposing undue systems/account management overheads.
- The absence of any features which would preclude use in small or large organisations, with equally variable numbers of differently-sized organisational units.

12.2.3 Mandatory requirements

B12.2 Tenderers are requested to provide their recommended requirements for the RKS and the expected upgrades during the first 5 years of operation, as part of their response in Part D – Schedule 8 – Software and Hardware.

12.3 Availability

The evaluation will consider the extent to which the proposed VERS RKS meets the following availability requirements:

- Prime time 99%
- Non Prime time 95%

Prime time is defined as Monday to Friday 8.00am to 6.00pm, except for recognised Victorian-wide Public Holidays.

12.3.1 Mandatory requirements

B12.3 Tenderers are requested to provide details of their system support as part of their response in Part D – Schedule 4.10 System Support.

12.4 Reliability

The evaluation will consider the extent to which the proposed process of developing the VERS RKS will result in a product that will not lose records irrespective of:

- Media failure (i.e. the destruction of media due to wear or accident)
- System failures (i.e. the complete failure of the system)
- Component failures (i.e. failure of components of the system)
- Communication failures (i.e. failures of transmission between components of the system)
- Disasters (i.e. fire, flood, etc)

12.4.1 Mandatory requirements

B12.4 Tenderers are requested to provide details of their system support and disaster recovery planning methodology as part of their response in Part D – Schedule 4.2 Methodology, Schedule 4.10 System Support, and Schedule 8 Software and Hardware.

12.5 Maintainability

The evaluation will consider the extent to which the proposed VERS RKS is easy to maintain over the long term, including:

- Availability of documentation and code to maintain the system and its components even if the original supplier no longer maintains them
- The use of tools and components in common use
- The maintenance of the capture components as new versions of the applications are introduced
- The management of software on desktop machines.

12.5.1 Mandatory requirements

B12.5 Tenderers are requested to provide details of their release strategy and change management methodology as part of their response in Part D – Schedule 4.2 Methodology and Schedule 4.9 Documentation.

12.6 Web enablement

The evaluation will consider the extent to which the proposed VERS RKS is Web enabled.

As described in the previous sections, user access to the Discovery system will be via the Web. This includes all searching, browsing, and display of records.

In addition, it is desirable that the management interfaces to the VERS RKS be accessible via a Web interface.

12.7 DOI Technical Environment

Tenderers should read the DOI Technology Architecture document for background information about the DOI Technical environment. The DOI Technology Architecture defines technology platforms, their interconnections, and the services that they must offer that provide an enabling platform for the work, application, and information architectures. This document does not dictate particular technology but the following guiding principle will be used to evaluate and rank responses.

The guiding principle is **REDUCE THE NUMBER OF ENVIRONMENTS**

- addresses limiting variations on products as a means of defining fewer 'common' environments to manage (cost) and operate (reliability)

Related policies:

- check the business system's natural fit to Notes/Domino before considering other development tools
- recognises the strategic nature Notes/Domino coupled with web-enabled deployment and inherent security capabilities
- check the business system's natural fit to Microsoft SQL Server before considering other database environments
- check the business system's natural fit to Microsoft Windows NT before considering other operating systems. NT is perceived as being capable of serving a diverse range of business system needs
- use Unix where Windows NT does not match business system requirements
- recognises the existing investment in infrastructure and skills surrounding Unix
- migrate systems from Unix to Microsoft Windows NT as they are replaced
- check the business system's natural fit to a thin-client deployment before considering other deployment models
- organisation regionalisation may result in duplication of operational environments

Any proposed solutions must be able to be integrated with the existing DOI environment.

12.7.1 Mandatory Requirements

B12.6 Recommendations on the most appropriate data storage mechanisms and media (considering both the initial implementation and potential scalability, as well as PROS 99/007) are required.

B12.7 Recommendations on the processor, memory, data storage requirements are required.

B12.8 Recommendations on appropriate backup mechanisms are required. Please state the expected duration of the backup using this mechanism and whether the backup can occur concurrently with the use of the RKS.

B12.9 Recommendations on deployment model are required.

B12.10 Statement is required of additional software required for development team.

B12.11 Statement of additional software required for testing, including user acceptance testing, is required.

B12.12 Statement is required of additional software required for production implementation.

B12.13 Recommendations on the hardware and software required for the training environment.

B12.14 Recommendations on the hardware and software required for the various test environments.

B12.15 Tenderers are to describe the software delivery mechanisms to be used.

B12.16 Tenderers are to provide a list of the complete set of software, versions, patch levels of software used, and a complete set of software, versions, patch levels of software required in the DOI infrastructure.

12.8 Development Environment

DOI prefers the outsourced model of system development. DOI recognises that transition issues are minimised if the development activity is conducted within the same environment as the eventual production environment. Therefore it is desired that all development activities be conducted at Nauru House, 80 Collins St. DOI will provide accommodation, furniture, office equipment, computers and software required by the development team.

12.8.1 Mandatory Requirements

B12.17 Tenderers are requested to provide a list of requirements for the development team in Part D – Schedule 3.6 Key Supports and also Schedule 8 Hardware and Software.

12.9. Data Migration

The Department of Infrastructure has many records, both paper and electronic. Part of the project will be to migrate the information about these records (and the records themselves if they are electronic) to the VERS RKS.

The sources of this information and records are:

- Recfind. DOI currently manages its folders and the records they contain within Recfind version 3.1.0B using the Btrieve database. There are currently (March 2000) 22 databases with the Recfind system, with approximately 250,000 documents and 156,000 folders. Most of these records are paper based. The Recfind database occupies approximately 2GBytes. During April and May 2000, DOI will be adding the records for the former Public Transport Corporation to the Recfind system. This will add approximately another 21,000 folders and 6,000 documents to the Recfind system. All of these records for the Public Transport Corporation are paper based. It will be necessary to extract the information about the folders and records and export it to the VERS RKS.
- Trim. The Land Monitoring Unit of DOI currently manages its folders and the records they contain within Trim 4.1. The system contains both paper and electronic records in an ISAM database. There are approximately 9,000 folders in the system of which 1,800 contain scanned images. There are approximately 45,000 scanned images held within this system. The Trim database occupies approximately 3GBytes of disk space. It will be necessary to extract the information about the folders and records and export it to the VERS RKS.
- Email. Most staff members within DOI have email messages that are records. It will be necessary to provide tools to export these records to the VERS RKS. It is anticipated that the export tool will allow users to map an email folder to a VERS RKS folder, and then to convert each email message in the email folder to a VEO within the RKS folder. Approximately 40 GByte of electronic mail is stored at any time. Up to 800 MByte of electronic mail per day is sent & received, or 16 GByte per month.
- File System. Many staff members have directories of (computer) files that are records. It will be necessary to provide tools to export these records to the VERS RKS. It is anticipated that the export tool will allow users to map a directory within the file system to a VERS RKS folder, and then to convert each file in the directory to a VEO within the RKS folder. Network File System disk space usage was estimated in March 2000 to be 250GByte with a growth of 10 GByte per month
- Lotus Notes. Lotus Notes is used extensively within the DOI to organise and hold digital information within work groups. It will be necessary to provide tools to export this information to the VERS RKS as records. It is anticipated that the export tool will allow users to map a Teamroom/Category/Subcategory to a VERS RKS folder, and then to convert each document as a record VEO within the appropriate RKS folder
- EDMS. DOI is rolling out Domino.Doc as an EDMS within the Department. It is anticipated that it will be necessary to migrate information from Domino.Doc to

the VERS RKS in a similar fashion to that required to migrate Lotus Notes documents to the RKS.

12.9.1 Mandatory Requirements

B12.18 Tenderers are requested to provide a separate costing for the migration of data from the existing Records Management Systems, Recfind and Trim as part of their response in Part D – Schedule 12 Tender Sum Information.

B12.19 Tenderers are requested to supply details of recommended data migration tools for migrating all information and records identified in section 12.9 above, as part of their response in Part D – Schedule 8.8 Recommended Data Migration Tools.