



[Released under the *Freedom of Information Act 1982*; FOI 27\_2016.]

## CER Information Management Policy

<b>This policy refers to:</b>	Information management policy
<b>Published date:</b>	04.05.15
<b>Date for review:</b>	01.07.16
<b>Application:</b>	
<b>Purpose:</b>	
<b>Owner:</b>	CER Chief Information Officer
<b>Contact:</b>	Shaun Keane
<b>Category:</b>	Information management

The electronic version published on the intranet is the current policy.

## Contents

CER Information Management Policy .....	1
1. Purpose.....	3
2. Policy statement.....	3
3. Scope .....	3
4. Context for information management .....	4
Legislation and Standards .....	5
Scheme specific legislation .....	5
5. Record management principles.....	7
Digital first .....	7
Record capture.....	7
Who captures records .....	7
Avoid duplication of records .....	7
Authorised information systems.....	8
Supporting information for records .....	9
Metadata definition .....	9
Secure and accessible records .....	11
Disposal of a record.....	12
6. Record keeping systems .....	14
7. Roles and responsibilities .....	14
8. Monitor and review .....	16
9. Authorisation .....	16
Attachment 1 – Summary of the record management principles.....	17
Digital first .....	17
Record capture.....	17
Who captures records .....	17
Avoid duplication of records .....	17
Authorised information systems.....	17
Supporting information for records .....	17
Secure and accessible records .....	18
Disposal of a record.....	18
Consultation .....	18
Endorsement.....	18
Approval .....	18
Version control.....	19

Related documents .....	19
-------------------------	----

## 1. Purpose

The purpose of this document is to establish the Information Management Policy for the Clean Energy Regulator (CER).

It supports the Clean Energy Regulator's regulatory requirements as an independent statutory agency under the *Archives Act 1983* and Australian Standard ISO 15489-2002 Records Management, thereby ensuring the Agency's recordkeeping practice is consistent with relevant Australian and international standards.

### Record/s definition

Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (AS ISO 15489.1 2002).

## 2. Policy statement

The Clean Energy Regulator's information and records are a vital asset that support ongoing operations. Therefore any information or record that enters, leaves or stays in the Agency will be subject to a common set of governance principles.

The Clean Energy Regulator will implement National Archives of Australia and Australian Standard ISO record keeping practices and systems in a fit for purpose manner that seeks to ensure the creation, maintenance and protection of accurate and reliable records.

All practices concerning recordkeeping in the Clean Energy Regulator are to be in accordance with this policy and its supporting procedures and guidance materials.

## 3. Scope

This policy applies to all of the Clean Energy Regulator's information and records, in any form, from any source and on any media. It applies to all staff and persons engaged by the CER as consultants and contract service providers collectively known as Clean Energy Regulator employees.

It also applies to all aspects of Clean Energy Regulator organisational business, all records created during business transactions and all business applications used to create records including email, office automation tools, database applications and websites.

Records and information created or received by the Clean Energy Regulator will generally remain in its custody and control. Externally sourced records and information, for example those captured as part of the investigations and litigation processes, will be managed in accordance with this policy and any Memorandum of Understanding (MOU) or inter-agency agreement until returned to their originating organisation.

This policy applies to:

- Electronic documents created by the Clean Energy Regulator, using desktop applications (e.g. Microsoft Office products such as Word, Excel, PowerPoint and Email).
- Audio visual materials.
- Electronic documents and information received and/or obtained by us (e.g. correspondence, applications, electronic transmissions, reports/submission, evidence).
- Image, graphics or text files.
- Portable Document Format objects, i.e. PDFs.
- Publications.
- Web and intranet content.

It provides the overarching framework for any other corporate or business recordkeeping policies, practices and procedures.

## 4. Context for information management

The Clean Energy Regulator supports a holistic approach to the management of all Agency information and seeks to integrate its information and recordkeeping policies and practices within the Agency's business operations and corporate processes.

### **Records Management definition**

The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes and maintaining evidence of the information about business activities and transactions in the form of records (AS ISO 15489.1 2002)

The Clean Energy Regulator governance framework for Information Management includes:

- considerations of business ethics, governance and stakeholder expectations of our behaviour
- understanding and publicising the importance of adequate recordkeeping management as evidence of corporate accountability
- embedding governance protocols into the day-to-day recordkeeping management processes
- implementing a strategy of continuous monitoring and review, and realignment of information management infrastructure and processes where needed
- developing systems that keep records and processes in a manner which meets our legislative obligations and business requirements
- incorporating risk assessment in the development of strategies and business requirements and rules for record management
- establishing a sound framework for records management based on national and international benchmarks and standards, and obligations for independent statutory agencies.

## Legislation and Standards

The Clean Energy Regulator will follow laws that relate to record management including:

- *Archives Act 1983*
- *Crimes Act 1914*
- *Electronic Transactions Act 1999*
- *Evidence Act 1995*
- *Public Governance, Performance and Accountability Act 2013*
- *Freedom of Information Act 1982*
- *Privacy Act 1988*
- *Public Service Act 1999*
- *Public Interest Disclosure Act 2013*

## Scheme specific legislation

- *Clean Energy Regulator Act 2011* or legislative instruments under that Act
- *Clean Energy Act 2011* or legislative instruments under that Act as preserved by the *Clean Energy Legislation (Carbon Tax Repeal) Act 2014*
- *Clean Energy (Charges—Excise) Act 2011* or legislative instruments under that Act as preserved by the *Clean Energy Legislation (Carbon Tax Repeal) Act 2014*
- *Clean Energy (Charges—Customs) Act 2011* or legislative instruments under that Act as preserved by the *Clean Energy Legislation (Carbon Tax Repeal) Act 2014*
- *Clean Energy (Unit Issue Charge—Fixed Charge) Act 2011* as preserved by the *Clean Energy Legislation (Carbon Tax Repeal) Act 2014*

- *Clean Energy (Unit Shortfall Charge—General) Act 2011* or legislative instruments under that Act as preserved by the *Clean Energy Legislation (Carbon Tax Repeal) Act 2014*
- *Carbon Credits (Carbon Farming Initiative) Act 2011* or legislative instruments under that Act
- *National Greenhouse and Energy Reporting Act 2007* or legislative instruments under that Act
- *Renewable Energy (Electricity) Act 2000* or legislative instruments under that Act
- *Renewable Energy (Electricity) (Large scale Generation Shortfall Charge) Act 2000*
- *Renewable Energy (Electricity) (Small scale Technology Shortfall Charge) Act 2010*
- *Australian National Registry of Emissions Units Act 2011* or legislative instruments under that Act

The Clean Energy Regulator will develop and maintain recordkeeping systems that capture and maintain records with appropriate evidential characteristics in accordance with the requirements of the above legislation. The Clean Energy Regulator recognises its obligations to be openly accountable for its actions under the *Public Service Act 1999*.

## Standards

Record management systems will be developed consistent with:

- The Australian Standard for Records Management (AS ISO 15489)
- The National Archives of Australia, AGLS Metadata Standard: Australian Government Implementation Manual, version 3.0, 2011.
- The Clean Energy Regulator's Enterprise Architecture, in particular the Data Reference Model that describes all the Clean Energy Regulator data assets for structured and unstructured data
- National Archives of Australia issued General Records Disposal Authorities and a Clean Energy Regulator Records Disposal Authority (RDA)
- A Clean Energy Regulator Business Classification Scheme (BCS) which will underpin file naming conventions
- National Archives of Australia Digital Transition Policy<sup>1</sup>
- National Archives of Australia guidance on Normal Administrative Practice (NAP) which allows for the destruction of records where the records are duplicated, unimportant or for short term use only,
- the Australian Government Investigations Standards that covers mandatory requirements for recording of referrals of breaches, investigations, witness statements and interviews
- Internal processes developed for Harradine Reports, requests under Freedom of Information Act (FOI), Australian Government Information Security Manual, Australian Government Protective Security Policy and Commonwealth Ombudsman investigation of complaints.

---

<sup>1</sup> <http://www.naa.gov.au/records-management/digital-transition-policy/index.aspx>

## 5. Record management principles

### Digital first

#### **Principle 1**

*Agency records are captured, stored and managed in digital form. Paper formats are considered an uncontrolled, convenience copy only.*

Where records are created or received in paper form, they are to be digitised in a way that enables the text to be fully searchable and indexed, and then stored in an authorised information system. The digital version then becomes the authorised record and the paper copy the uncontrolled, convenience copy.

Where there is a requirement to manage records in paper form, the Division Head must grant an exception on a case-by-case basis. The reference to the paper record must still be managed as a digital object in an authorised information system and the security of the physical object managed appropriately in accordance with its security classification and/or Limiting Markers where required.

All digital records should be text-searchable to enable easy discovery for others, particularly where FOI and auditing is concerned.

### Record capture

#### **Principle 2**

*Where evidence is required of a decision, action or business transaction a record must be captured.*

### Who captures records

#### **Principle 3**

*The person creating a document is responsible for its capture as an Agency record.*

*The person receipting client information or business information, as part of a business process, is responsible for its capture as an Agency record.*

### Avoid duplication of records

#### **Principle 4**

*Records should be captured and stored once.*

*Final internal versions and original versions received from external parties should be maintained in unaltered form*

“Final” versions of records, or information received from external sources, must not be modified. They are to be maintained in the form they were finalised or received as unaltered records.

When it is proposed to make any additions, changes or annotations to a record this must be done on a copy of the record. The copy becomes a new record in its own right, and is required to be captured as a new digital record.

Example 1: A print is made of an email and the print is annotated as a result of a business action, it should be captured as a new record.

Example 2: A print copy is made of a policy in digital format in the EDRMS and reviewed in its paper format. The copy must now be captured as a new record and stored in the EDRMS.

Example 3: A copy of a record in the EDRMS is made and worked on outside the EDRMS in collaboration with stakeholders outside the Clean Energy Regulator. The new version must now be captured and stored in the EDRMS as a new record.

Internal distribution of an electronic record can be done by sending (e.g. via email) a link to the record in the central electronic store, rather than sending copies to other people.

Reliance on hard copy records should be minimized. Where hard copies are used, they should be clearly labelled 'copy', and subsequently destroyed under normal administrative practice.

Copies of documents received in legal proceedings, unless otherwise ordered by the court or tribunal must not be deleted, even if they are a duplicate of records. This is to ensure that the agency has a complete record of what has been distributed or received in the course of litigation..

## Authorised information systems

### ***Principle 5***

*Records must be captured into and controlled using an authorised information system.*

The record should be captured into the appropriate authorised information system at the time of creation or receipt, along with the information that supported or informed the decision, actions or business transaction. These authorised information systems are to be used by Clean Energy Regulator employees to ensure that:

- Corporate records and information are routinely captured on creation or receipt.
- Access to records and information is enabled for as long as required and is appropriately managed.
- Records and information are protected from unauthorised alteration or deletion.
- Records disposal is in accordance with Records Disposal Authorities issued and/or approved by National Archives of Australia as part of an approved business process or in accordance with Normal Administrative practice (NAP).
- There is one authoritative and primary source of information about the organisation's decisions and actions documented in its records.

Authorised information systems currently used by the Clean Energy Regulator include:

- Aurion – HR records.



- TechOne – Financial records.
- Slipstream – Records relating to Ministerials and Briefs.
- EDRMS – Corporate and business records.
- CRM – Stakeholder information.

## Supporting information for records

### *Principle 6*

*Record capture will include the attachment of descriptive information (metadata) about the record's context.*

### Metadata definition

Information describing context, content and structure of records and their management through time (AS ISO 15489.1 2002).

Capture of a record into an authorised information system involves processes that prove the record's existence and context. In some cases this will be done automatically by the system.

The baseline metadata for any record must encompass:

Property	Mandatory/Optional	Description
• Unique identifier	Mandatory	System driven
• Description	Optional	Free text
• Date created	Mandatory	Date of the finalised record
• Date modified	Mandatory	Date of the last modification to the record where the versions are in draft
• Author, sender or recipient	Mandatory if an email	Text
• Document creator	Mandatory	Text, based on Active Directory record
• Physical form	Mandatory, where it refers to a physical object	Text based on a reference to the physical object

• Physical location	Mandatory, where it refers to a physical object	Text based on a reference to the physical object
• Digital location	Mandatory, where it refers to a digital object	Text, reflecting the placement/hierarchy in the information system's logical structure
• Classification	Mandatory	Text, according to the Business Classification Scheme (BCS)
• Related records	Optional	Links to related record
• Business system	Optional	Location from which the record was captured
• Software	Optional	The software/application that is required to open the object
• Security classification	Mandatory	As described in the PSM
• Limiting Marks	Optional	As described in the PSM
• Records Authority	Mandatory	Actions to occur in relation to that record

Metadata ensures that important details about the Clean Energy Regulator's information is recorded in a structured way, and provides valuable context to the information. It also:

- Provides a tool for the control and management of records and other information resources
- Provides a means of verifying the authenticity and integrity of records and information
- Assists in the discovery and retrieval of information
- Allows the capture of technical details about information resources, enabling them to be rendered and read

Without metadata, information and records have no context, making them difficult to find, retrieve and use.

Additional metadata for business areas can be captured in Clean Energy Regulator documents as required.

## Secure and accessible records

### **Principle 7**

*Conditions and controls must be in place to make records and information secure and accessible.*

Access restrictions are based on the need to protect, among other things:

- Confidential and/or protected information
- Sensitive enforcement and compliance activities/information
- Legal professional privilege
- Intellectual property of the Clean Energy Regulator and other parties
- Individual privacy

Access to records and information may be tracked by the authorised information systems to:

- Ensure records and information are seen or used by authorised users
- Show patterns of usage for system and process audit.

Appropriate storage conditions and controls must be in place to ensure that records and information are protected, accessible and managed in a cost effective manner. This applies to storage of current records and information in use, and to inactive records and information that must be kept for designated periods.

Storage options are determined on the basis of:

- Retention requirements under Records Authorities issued by the National Archives of Australia
- Volume and growth rate of records
- Record media
- Findability, use and retrievability of the records and information
- Security requirements and classifications
- Cost of storage
- Access needs.

Storage of electronic records is subject to additional processes to prevent their loss and to ensure retention for the required periods. This includes:

- Regular backup routines
- Offsite backup storage
- Maintenance processes such as copying or migration to prevent data erosion, or to counter software or hardware obsolescence.
- Clean Energy Regulator Disaster Recovery Plan.

ICT Security is responsible for maintaining individual and group security and access permission profiles (in accordance with the IT Security Policy Framework).

**Vital Records definition**

Records without which an organisation could not continue to operate. Those records containing information needed to re-establish the organisation in the event of a disaster (National Archives of Australia, Recordkeeping Glossary, 2004).

Vital records are subject to additional management and storage controls as prescribed by business rules the Clean Energy Regulator Disaster Recovery Plan.

## Disposal of a record

**Principle 8**

*Records must be disposed of in accordance with the relevant Records Authority and according to the Clean Energy Regulator Normal Administrative Practice (NAP) procedures*

The Records Authorities issued by National Archives of Australia must be used to govern the destruction, deletion, retention or transfer of records.

**Records Authority definition**

A formal instrument that defines the retention periods and consequent disposal actions authorised for classes of records described in the authority. These are issued to individual agencies by the National Archives of Australia and cover agency specific core business.

Records can also be destroyed under Normal Administrative Practice in accordance with National Archives of Australia's guidelines.

### **Normal Administrative Practice definition**

A practice which allows agencies to destroy certain types of records in the normal course of business, without express authorisation from National Archives of Australia (National Archives of Australia, Recordkeeping Glossary, 2004).

Documents not required to be captured into authorised information systems are those of a transitory nature, that are duplicated, unimportant, that are not needed for ongoing business, and would not be needed by any other person in the organisation. These records may be disposed of under normal administrative practice.

The Information Management team will provide advice and assistance on the use of the approved Records Authorities. All Records Authorities apply to hardcopy and electronic records. A manual disposal implementation process is required annually for hardcopy records. For electronic records the Records Authorities will be embedded into EDRMS for automated flagging of records for destruction or other action.

All disposal action as authorised by the Records Authorities must be suspended if a Disposal Freeze is issued by National Archives of Australia or a Hold Order is issued by the Clean Energy Regulator management.

All records destruction, transfer and retention action are to be done in conjunction with the Information Management team to ensure corporate compliance and governance requirements are met. This will include:

- Authorisation of disposal action (in accordance with Records Authorities)
- Appropriate methods of physical destruction, and documentation of destruction action
- Arrangements for transfer of records and information to alternative media
- Arrangements for physical transfer to storage and documentation of transfer details.

Records left by employees who leave or move within the Agency are transferred to the successive person undertaking that role or function, or disposed of in accordance with a Records Authority approved by National Archives of Australia under prescribed procedures.

Records held by external organisations or designated persons that have ceased to provide a service to the Clean Energy Regulator will be transferred back into our custody and either:

- Integrated into the relevant authorised system , if still current
- Treated in accordance with the records authorities and related processes, if not current.

Original and/or scanned images of documents that have been compelled under statutory notice or subpoena are to be disposed of in accordance with a *Clean Energy Regulator Records Authority* and in reference to the *Evidence Act*.

A snapshot summary of these policy principles is at Attachment 1.

## 6. Record keeping systems

A record should be created when a document is drafted or when information, received from an external source, is receipted.

Printing the record to paper creates an uncontrolled, convenience copy. Where annotations are added to the uncontrolled copy and a new record created, this must be captured in the appropriate information management system.

The EDRMS manages the following processes:

- Creation or capture of information and records
- Storage of information and records
- Protection of information and record integrity and authenticity
- Security of information and records
- Access to information and records
- Disposal of information and records – in general, it is an offence to destroy any Commonwealth record without authorisation from the National Archives of Australia. Unless otherwise authorised, all record disposals within the Clean Energy Regulator must be undertaken in compliance with the organisation's approved Records Disposal Authority, and relevant General Disposal Authorities issued by the National Archives of Australia.

The Clean Energy Regulator's record management systems are dedicated to the creation and maintenance of authentic, reliable and usable records which meet the needs of internal and external stakeholders.

All of the Clean Energy Regulator's records will be created and maintained within the preferred record management systems outlined above or as specified by the Information Management section. Records must not be stored in G and H drives, hard drives or Temp Docs. These facilities do not contain record management functionality to ensure that records will be appropriately captured, maintained, versioned, and backed-up. They are, therefore, unable to provide access to, and evidence of, business activities over time.

Wherever possible, records are to be kept in a text searchable format that is easily searched, retrieved and distributed to internal and external parties as and when required (for example as the result of Freedom of Information requests, subpoenas and orders for production to courts and tribunals).

## 7. Roles and responsibilities

The Chief Executive Officer of the Clean Energy Regulator will:

- Authorise the Record Management Policy

- Provide sufficient support and resources for ensuring records management requirements can be addressed
- Promote compliance with the Clean Energy Regulator's record management policies and procedures to all Clean Energy Regulator employees.

The Chief Information Officer will:

- Develop strategies to support the Record Management Policy
- Ensure that the Clean Energy Regulator's record keeping practices comply with its obligations and responsibilities as an independent statutory authority
- Oversee the alignment of record management functionality with Clean Energy Regulator record keeping policies and business requirements.

The Information Management section will:

- Assist the Chief Information Officer to develop strategies supporting the Record Management Policy
- Create and maintain information and record management policies and procedures documenting the Clean Energy Regulator's record management requirements and containing recordkeeping rules and practices that all Clean Energy Regulator employees are obligated to follow
- Promulgate the Clean Energy Regulator's record information and management policies and procedures to all Clean Energy Regulator employees
- Deliver record management training and advice to Clean Energy Regulator employees
- Implement processes for mandatory government information and record management requirements, for example, Harradine Reports, National Archives of Australia Check Ups, National Archives of Australia Disposal Freezes and the Digital Transition Policy
- Maintain, monitor, review and report on the Clean Energy Regulator's record management systems
- Ensure that the General Records Authority, Records Disposal Authority and other National Archives of Australia and Australian Standards for recordkeeping are effectively implemented in the Clean Energy Regulator record management systems and applications where Clean Energy Regulator information is stored.

The IT Branch and EDi System Administrators will:

- Maintain the technology used to support systems that capture and keep records electronically ensuring that all documents are reliable, available and accessible to staff when required.

All Managers and Supervisors of Clean Energy Regulator employees will:

- Assist the Chief Information Officer to develop strategies supporting the Record Management Policy
- Monitor staff under their supervision to ensure that they understand and comply with the Clean Energy Regulator's record management policies and procedures for the creation and maintenance of records

- Support and foster a culture within their workgroup that promotes good record management practices.

All employees will:

- Attend training to understand the record management obligations and responsibilities that relate to their roles
- Adhere to Clean Energy Regulator policies, procedures and standards in records management, documenting their daily work, and specifically create and capture records into the Clean Energy Regulator's record management systems
- Only destroy records under an authorised records authority or through the application of normal administrative practice.

The above responsibilities also apply to visitors who have been granted access to Clean Energy Regulator Records and information.

## 8. Monitor and review

Clean Energy Regulator employee and system compliance with this policy will be regularly monitored to:

- Ensure that records will be accepted as evidence of Clean Energy Regulator business, if and where required
- Ensure that the policy is working to improve the Clean Energy Regulator's performance
- Ensure that records and information management procedures and processes are working effectively, meet the required outcomes and that Clean Energy Regulator employees are effectively and efficiently using the authorised corporate systems for records and information management
- Ensure that the Clean Energy Regulator's information systems for records and information management are operating continuously and reliably.

This policy is scheduled for review by March 2015. This review will be conducted by an internal review process established by senior management.

## 9. Authorisation

This policy is issued under the authority of the Chair and Chief Executive Officer of the Clean Energy Regulator.



# Attachment 1 – Summary of the record management principles

## Digital first

### *Principle 1*

Agency records are captured, stored and managed in digital form. Paper formats are considered an uncontrolled, convenience copy only.

## Record capture

### *Principle 2*

*Where evidence is required of a decision, action or business transaction a record must be captured.*

## Who captures records

### *Principle 3*

*The person creating a document is responsible for its capture as an Agency record.*

*The person receipting the client information or business information as part of a business process is responsible for its capture as an Agency record.*

## Avoid duplication of records

### *Principle 4*

*Records should be captured and stored once.*

*Final internal versions and original versions received from external parties should be maintained in unaltered form.*

## Authorised information systems

### *Principle 5*

*Records must be captured into and controlled by an authorised information system.*

## Supporting information for records

### *Principle 6*

*Record capture will include the attachment of descriptive information (metadata) about the record's context.*

## Secure and accessible records

### *Principle 7*

*Conditions and controls must be in place to make records and information secure and accessible.*

## Disposal of a record

### *Principle 8*

*Records and information must be disposed of in accordance with the relevant Records Authority and according to Clean Energy Regulator Normal Administrative Practice procedures.*

## Consultation

Internal stakeholders:	
External stakeholders:	

## Endorsement

Endorsed on:	04.05.15
By:	Chief Operations Officer
Signature:	

## Approval

Approved on:	
By:	
Signature:	
Period of effect:	
Review date:	

## Version control

Version	Date	Author	Approver
0.1	13/2/2013	J. Manley	Draft for Agency consultation
0.2	21/02/2013	J.Abbey	Style formatting
0.3	21/03/2013	J. Manley	Incorporating stakeholder and Delivery Division EGM comments
0.4	28/03/2013	J.Manley	Incorporating minor amendments from Steering Committee
1.0	18/03/2013	J Manley	Endorsed by Senior Leadership Team
1.1	01/10/2014	G Wyatt	Adjust for digital records and deprecate paper records
1.2	09/10/2014	G Wyatt	Completion of Draft
1.3	13/10/2014	G Wyatt	2 <sup>nd</sup> Draft
1.4	17/11/2014	G Wyatt	Dependable Services ORG changes
1.5	08/04/2015	G Wyatt	Communications change to new corporate livery
1.6	28/04/2015	A Hilson	Updates following EGM review
2.0	04/05/2015	A Hilson	Endorsed by Chief Operations Officer

## Related documents

Document Title	Location
Information Management Strategy	<a href="http://edi/ict">http://edi/ict</a>
Good Decision Making Guide	<a href="http://cerintranet/about/standard-operating-procedures/Documents/Guide to Good Dec Making V3.docx">http://cerintranet/about/standard-operating-procedures/Documents/Guide to Good Dec Making V3.docx</a>
Information Security Strategy	<a href="http://cerintranet/news/staff/Pages/Information-Security-Strategy-issue-24.aspx">http://cerintranet/news/staff/Pages/Information-Security-Strategy-issue-24.aspx</a>
Information Security Policy	<a href="http://cerintranet/information/security/Pages/Information-Security.aspx">http://cerintranet/information/security/Pages/Information-Security.aspx</a>
Information Security Enterprise Architecture	
Overview of the Enterprise Warehouse	
Client Engagement Strategy	<a href="http://cerintranet/about/Documents/Client Engagement Strategy.docx">http://cerintranet/about/Documents/Client Engagement Strategy.docx</a>

Fraud Control Plan

<http://cerintranet/governance/risk/Documents/2014 Fraud Control Plan.docx>