Managing Records as Reliable Evidence for ICT/ e-Government and Freedom of Information

Rwanda Court Case Study



International Records Management Trust

August 2011

**Contents**

|  |  |
| --- | --- |
|  | Page |
| Introduction | 2 |
| The Court in the Judicial Structure | 2 |
| ICT in the Judiciary | 3 |
| Records Management in the Judiciary | 3 |
| Records Management Integration with Case Management Systems | 5 |
| Conclusion | 14 |

**Introduction**

The purpose of the court case studies is to examine the manner in which the courts are handling records management in the electronic environment. The study covers five East Africa member countries in: Burundi, Kenya, Rwanda, Tanzania and Uganda. This case study was undertaken at the Supreme Court of Rwanda.

**The Court in the Judicial Structure**

***Ministry of Justice***

The Ministry of Justice oversees the justice sector and ensures collaboration between various judicial sub-sectors. Institutions operating under the auspices of the Ministry of Justice are linked by a common mission (Justice Vision of the Country) but are operationally independent and responsible for monitoring their own programmes and fulfilling their own mandate.

***Supreme Court***

The Supreme Court’s remit is defined in constitutional article 144 designating the court the highest jurisdiction in the country, responsible for co-ordinating and overseeing court and tribunal activities while ensuring the independence of the judiciary. The decisions of the Supreme Court are final and are not subject to appeal except in instances of petitions of mercy or revision of a ruling. Aside from the Supreme Court, Article 143 of the Constitution also establishes the following courts:

* the High Court
* the High Commercial Court
* the Commercial Tribunals
* the High Instance Tribunals
* the Grass-roots Tribunals.

***Ordinary Courts***

The High Court's primary offices are located in the city of Kigali, but the court has jurisdiction over the entire country, except where the law stipulates otherwise. The Court's mandate, operations and structure are defined in law N° 51/2008. The High Court has four regional courts, located in Musanze, Nyanza, Rwamagana and Rusizi, which hear cases and provide judgments on matters within their respective jurisdictions. Each of the regional courts is overseen by a president, who reports directly to the President of the High Court.

***Intermediate Courts***

The mandate of the Intermediate Courts is defined in law N° 51/2008; they are responsible for trying civil and criminal cases. They include a number of specialised chambers, some to provide judgments on cases involving minors, others to try administrative and social matters.

**ICT in the Judiciary**

The Supreme Court and Judiciary have developed their ICT projects in conformity with the National ICT Policy and the National Information Communication Infrastructure. This necessitated the establishment of an internal ICT Department to oversee the proper operation and implementation of ICT systems. The ICT Department is led by a Director General, who is assisted by six system administrators and IT technicians. The Director General oversees and manages all IT related court services in addition to supervising and liaising with IT personnel working in other parts of the court system.

The ICT Department ensures that standardised office systems are in use across the Supreme Court. They are also responsible for overseeing overall compliance with Judiciary ICT policies, such as the One-Person-to-One-Computer Policy, whereby employees are entitled to a computer with Internet connectivity. Employees in courts located up-country are supplied with modems to facilitate access and ease of communication with the central offices in Kigali.

The Supreme Court recently introduced a court recording and transcription system in five courtrooms, with funding from the Investment Climate Facility for Africa. Since the initial implementation, the recording system has been introduced into four other courts: the High Court, the Commercial High Court and two provincial high courts. In response to the national e-Governance plan, the court also implemented a website to act as an information dissemination tool enabling citizens to access information on rulings and courts procedures.

**Records Management in the Judiciary**

The records management function falls under the purview of the Supreme Court Registry, which is under the authority of the Chief Registrar. One of the primary responsibilities of the Chief Registrar is ensuring proper case file management in the Court. More specific functions of the Chief Registrar include:

* keeping minutes of all proceedings, maintaining court registers and managing the list of open and closed cases
* notifying and preparing parties for their hearing
* preparing draft verdicts or rulings, when necessary
* establishing, at the beginning of every calendar year, an alphabetical list of all the decided cases, including a summary of the subject matter of each of the claims
* creating a list of accused persons in criminal cases including a summary of the chargeable offences and the court's final ruling on the case.

The Court Registry is responsible for administering current and semi-current paper and electronic records produced by the court. Semi-current records are transferred to an archives centre located at the Supreme Court and administered by an archivist under the supervision of the Registrar. To facilitate the management of the current and semi-current records, the Registry has developed an internal records management procedure manual to guide staff in the proper care and management of case files. There is no manual for managing electronic records.

The Supreme Court has acknowledged the need for records management to facilitate efficient operations and to optimise service delivery. In 2009 it initially used a case management system called Judicial Document Register which was eventually rolled out to the lower courts, but unfortunately it did not meet all the functional needs of the Courts. In June 2010 a new system, FinDoc, was implemented, which includes case management and electronic document management functionalities. It is hoped that the new system will improve workflow and document retrieval. FinDoc, which is in the final stages of implementation, allows registrars and judges to consult digital court case files.

There are plans to implement FinDoc in 22 courts. The Supreme Court also has initiated a digitisation project aimed at facilitating access and retrieval of all court judgments. Although the system allows users to capture, retrieve and search court records, it does not, at present, include records management functionalities such as classification schemes, file management or retention scheduling.

Another information management system being considered for the Judiciary is a human resource management programme that is being developed at the Ministry of Public Service and Labour. Currently management of personnel files is done manually. The new software programme would allow for greater accountability and efficiency in the management of personnel files. Once the system is in place at the Ministry of Public Service and Labour, there are plans to roll it out to other government institutions such as the Supreme Court.

**Records Management Integration with Case Management Systems**

***Assessment***

*Project Initiation*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| Records management issues are identified and documented when the need for an ICT/ e-Government system is identified and documented. | * Records management issues have been identified and documented * All ICT/ e-Government projects include a clear statement on addressing records management requirements. | Records management issues have been identified and but not well documented principally due to lack of competence and skills.  No, ICT/ e-Government projects do not include a clear statement on records management, rather the emphasis is on document management with little or no reference to records management.  The need for records management is felt at the national level which is why there is a project underway to draw up a records management policy at the National level. |

*Planning*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| The analysis of business needs includes records management issues; potential solutions incorporate records management considerations. | * A business needs analysis has been carried out * The analysis includes a consideration of records management issues. | Yes, but little consideration was given to records management issues especially regarding classification and retention plans. |
| In assessing risks associated  with the potential solutions, risks associated with records management are also taken into account. | Risks associated with records management in the potential solutions have been assessed and documented. | Not well taken into account. |

*Requirements Analysis*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| An analysis has been conducted  of the records management  requirements for the ICT/ e-Government system based on the records management issues identified during the planning stages. | An analysis of the records management requirements of the ICT/ e-Government system has been conducted and documented. | There was no proper analysis of records management requirements, rather emphasis has been placed on document management functions such as records capture, workflow and records preservation. |
| The analysis of records management requirements for the ICT/ e-Government system makes reference to internationally recognised standards. | The analysis makes reference to international records management standards or other internationally recognised sets of requirements (eg, ISO 15489, MoReq, DoD 5015, DIRKS, etc). | No, since there was no proper analysis of records management requirements, there is no reference to internationally recognised standards. |

*Design*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| The points in the process where records are expected to be generated and captured are defined and reflected in the functional requirements of the ICT/ e-Government system. | * All transactions that result in the creation of records within the ICT/ e-Government system have been defined and documented * A mechanism is in place to ensure that all records created within the ICT or e-Government system are effectively managed as evidence of transactions. | * Yes, records’ creation have been clearly defined and documented. * Yes, document management system (FinDoc) is being implemented. |
| Performance measures are developed for addressing the records management performance of the ICT/ e-Government system. | Performance measures are in place to assess the ability of the system to meet records management requirements. | Not yet developed. |
| The system creates an audit trail that keeps a complete history of the creation, use and retention of all records within the system. | The system captures metadata and creates an audit trail to provide a complete record of the creation, use and retention of records within the system. | Yes, the system creates an audit trail that captures use, modification and deletion although no retention rules are presently applied to records. |
| Performance measures are carried out regularly to assess the ability of the system to meet records management requirements. | The system’s records management performance has been assessed within the last 12 months. | Yes, the performance measure are done regularly on the old case management system however the new one is still being implemented and performance measures are not in place. |
| A designated member of staff has been assigned responsibility for monitoring the system audit trail. | Responsibility for monitoring the system audit trail is documented and assigned to a designated member of staff. | All the system’s roles are assigned to the system administrator who is the ICT Manager. |
| The audit trail is analysed regularly to monitor access to the system, changes to access and security controls, and the integrity of records within the system. | The system audit trail has been analysed within the last 12 months. | No audit trail analysis has been made yet as the system is still being implemented. |

*Implementation*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| The developed system has been tested for its records management performance against technical, management and functional records management requirements. Testing included a ‘live’ test in an operational context. An acceptance test has been conducted to confirm that the system meets records management requirements. | Acceptance tests have been carried out for records management requirements; acceptance tests for records management requirements may be separate or incorporated in acceptance tests for the whole system. | A live demonstration was done for a few requirements; capture, search, retrieval but other critical records management requirements like a functional classification plan, file management, retention, box management, life cycle management, Reports, etc were not demonstrated. |

*Maintenance*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| Mechanisms have been established to assess system compliance with records management requirements through time. | There is a documented mechanism for assessing the system for compliance with records management requirements; compliance assessment for records management requirements may be separate or incorporated in compliance assessment for the whole system. | No mechanism in place so far, may be after the implementation but it is unlikely to be effective since most of the records management requirement have not been taken into account. |
| Assessments for system compliance with records management requirements are regularly carried out. | An assessment for records management compliance has been carried out in the last 12 months. | None so far for the new system since the system is being implemented, but system compliance assessment would be difficult given that not all records management requirements have been identified and documented. Neither has the assessment been identified as a need. |

*Review and Evaluation*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| There are performance standards to assess whether the ICT/ e-Government system meets records management requirements, for example in relation to records security, data quality and data completeness. These may be separate record management standards or systems standard that include records management standards. The standards should be related to records management requirements. | There are documented performance standards to measure whether the ICT/ e-Government system meets records management requirements. | There are no records management performance measure standards for the ICT/ e-Government system as records management practices and methods were not part of the system’s planning process. |
| Performance assessments are conducted to assess the system’s compliance with records management standards. | A performance assessment has been carried out to assess the system’s compliance with records management standards within the last 12 months. | There has not been any performance assessment carried out so far. The system is still being implemented. |

*Creating and Capturing Records*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| *The system must be capable of:* |  |  |
| Capturing records in all formats as well as converting records from one format to another if required. |  | Yes the system ( Fin Doc) has the capacity to capture records in all formats as well as converting records from one format to another as required. |
| Assigning unique identifiers to the records that will remain unchanged as long as the records exist. | It is not possible to assign the same number to two records. | Yes, it gives unique identifiers through its indexing tool. |
| Supporting and applying security and access controls during the process of capturing records to ensure that the records are protected from unauthorised access, alteration  and destruction/ deletion. | Access controls are automatically or manually assigned to complete the creation and capture of a record. | Yes, security and access controls are manually assigned to ensure protection of records. The IT department is charged with this task. |

*Managing and Maintaining Records*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| *The system must be capable of:* |  |  |
| Validating metadata, for example against a range of predefined values such as a classification scheme. | The system is designed to control the selection of metadata from pre-defined values (eg, in relation to classification of records). | Classification plans are  not defined/ designed  in the new system and  therefore it is not possible to validate metadata against a range of predefined values such as  a classification scheme. |
| Creating rules to control the  selection of metadata. | The system has the functionality to create rules to control the selection of metadata (eg, in relation to classification of records). | Yes, it is possible to control selection of metadata. |
| Assigning appropriate retention and disposition rules to records during record creation. | To complete the creation and capture of a record, a retention rule must be assigned. | There are no records retention rules. |
| Creating and maintaining an audit trail that tracks user access to records contained within or managed by the system. | There is an audit trail that tracks access to the records contained within or managed by the system. Whenever a user accesses a record, audit metadata is created. This audit metadata includes at least the date and time of access and the user’s ID. | System records all users’ actions to allow administrators to trace changes made on a document or by specific user. |
| Creating and maintaining an audit trail that tracks changes to records and record metadata. | The audit trail captures any changes made to records or metadata contained within or managed by the system. | System records all users’ actions to allow administrators to trace changes made on a document by specific user. |
| Providing an easy method of checking the audit trails for changes to records and records’ metadata within the system. | A system audit is carried out every six months. This audit examines the audit trail for any changes made to records and records’ metadata. | No audit trail analysis has been conducted so far but it is a responsibility of the IT Department. |

*Managing Hybrid Records*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| *ICT systems that manage hybrid records must be capable of:* |  |  |
| Searching for and retrieving all physical, hybrid and digital records registered by the system. | System rules are consistent for physical, hybrid and digital records (eg, records are labeled or described for searching and retrieval purposes). | FinDoc is capable of managing a hybrid records environment. |

*Searching, Accessing and Retrieving Records*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| *The system must be capable of:* |  |  |
| Retrieving and listing a set of digital records and associated metadata that meet the search criteria. | At least two criteria may be used to search for records in the same system, either using the record content or its metadata (eg, unique identification number, date of creation and capture, record type, user ID of creator). | The system provides powerful full-text search capability by keyword —based on the defined attributes—including scanned documents. You can also retrieve records based on unique numbering system that corresponds to the case file number. |
| Restricting the definition and  maintenance of access and security controls to an authorised system administrator. | Responsibility for managing access controls is assigned to a designated member of staff or office. | Yes, access is controlled by the system administrator who is responsible for assigning user IDs and passwords for various access levels |
| Supporting central management of access and security controls; applying these controls to users, records and associated metadata. | There are documented standards and procedures for applying system access controls. | Yes, the system has this capability. |

*Records Retention and Preservation*

| **Good Practice Statement** | **Indicator** | **Findings** |
| --- | --- | --- |
| *The system must be capable of:* |  |  |
| Providing backup for all records and the records’ metadata within the system. | * There is a daily backup of all system data * The backup is stored externally from the main system. | * Backup done every three months * Yes, backup on CDs and external hard discs. |
| Enabling an authorised individual to create, maintain, modify and manage retention and disposition rules. | A designated member of staff or office has documented responsibility for managing retention and disposition rules. | Not so far, the system has the capability to support this feature but retention and disposal rules have not been either applied or updated. |
| Applying retention instructions to records and triggering the appropriate disposition event when the retention period expires. | There are documented policies and procedures for assigning retention and disposition instructions to records. | There are no documented policies and procedures for assigning retention and disposition instructions to records as identified |
| Creating an audit trail of records retention and disposition rules and actions; enabling an authorised individual to carry out regular audits. | There is a documented audit of records retention and disposition rules and actions at least every 12 months. | No. |

*Retaining and Disposing of Records*

|  |  |  |
| --- | --- | --- |
| **Good Practice Statements** | **Indicator** | **Findings** |
| *The system or application must be capable of:* |  |  |
| Capturing information in a  structured format so as to  create an electronic record. |  | The IT department is tasked with this. |
| Connecting with an ICT system that has integrated records management functionality, as set out in Category 3, in such a way that records are captured and managed effectively.  Connecting with an ICT system designed specifically for records management (eg an EDRMS) in such a way that records are captured and managed effectively. | Records generated through the e-Government system or application are present in the ICT / records management system. | Connecting with an ICT system that has integrated records management functionality, as set out in Category 3, in such a way that records are captured and managed effectively. This is the daily work of the IT department and the court clerks. |

***Analysis***

FinDoc has many features that could assist the Supreme Court in managing its records to ensure the long-term viability and validity of court records. Strong audit trail capabilities enable the IT Department, which is tasked with monitoring the system’s security and integrity, to prevent unauthorised access, modification and deletion. However, an audit trail must be monitored and at present there is no audit trail monitoring procedure in place. This could compromise records integrity due to undetected unauthorised document access.

There are then issues to consider in relation to planning and implementing the system. The Court carried out a business needs analysis and noted that proper information management was a necessity. However it did not sufficiently take into account good practice in records management. No risk analysis or records management functional analysis was conducted to determine whether the system met international standards.

The system is designed to capture, retrieve and preserve information, but classification, file management and retention scheduling have not been adequately addressed. Without integral elements such as classification schemes, records are difficult to retrieve, even with unique identifiers and search functionalities. Records identifiers only allow users to find one document at a time, whereas general search functions will retrieve all relevant records based on keyword searches, requiring the user to parse through the material and find the relevant records. With a records management classification scheme, users are able to find all the records that comprise a given business transaction, making it easier when auditing decision-making processes. Without a cohesive and standardised records classification scheme with appropriate retention rules, information can easily be destroyed inadvertently.

Another issue to be addressed is the frequency of system back-ups. Presently, back-ups are conducted on a quarterly basis, meaning that if the system fails masses of vital electronic information could be lost and/ or corrupted, which would compromise court processes and affect citizens’ ability to assert their rights.

**Conclusion**

The Judiciary has made considerable headway in building its ICT infrastructure, in particular by implementing FinDoc. Although the system could potentially support records management functionality no assessment has been carried out to determine its effectiveness in managing the information needs of the Court’s. Consequently records can be difficult to retrieve and can be lost or destroyed.

The Supreme Court of Rwanda understands the critical need to manage information properly, especially as documents are the basis of evidence. Without planning for records management controls, the Court is at risk of compromising the evidentiary value of records that are needed to attest to court transactions and processes. This would have a serious impact on the timely administration of justice for litigants.