

# RECORDS MANAGEMENT COURSE

Presented by Alison Lee (CCASA CEO & Director of Lee's Legal Compliance Solutions)



30 September 2021



8:30 - 16:00



Online via MS Teams



For any organization, keeping records is essential in its day-to-day operations. In the modern business world where almost everything is captured and stored online, it can be an overwhelming task to sort through and retrieve data and records. Records must be properly managed from the time when they are created, stored, accessed, and updated until they are archived for future reference. The importance of maintaining an effective record management system cannot be over-emphasised.

## So how is this done?

In order to effectively manage records, an organization must develop and implement an effective records management program and a set of related procedures.

## But what is Records Management?

Records management is the professional practice or discipline of controlling and governing what are considered to be the most important records of an organization throughout the records' life-cycle, which includes from the time such records are conceived through to their eventual disposal.

## What will the course cover?

This course will assist you in understanding the nuts and bolts which make up a records management system and give you directions on how to develop and implement an effective records management program.

Areas which will be covered over the one-day workshop include:

- **The legal framework:** laws regulating records and the management thereof;
- **The implications of this legislation and how to ensure compliance:** the legal how of records management;
- **Records creation:** rules on how to create and classify a record according to a file plan;
- **Records storage:** rules on how to save and store a record;
- **Records sharing:** rules on who has access to a record and how such access or sharing is managed;
- **Records retention:** rules on record archiving;
- **Records destruction:** rules on the destruction of a record;
- **Litigation hold:** procedures and scenarios;
- **Safety and security:** IT, ISO and POPIA requirements and how to ensure records are safe and secure;
- **Preservation of Records:** understanding where appropriate and setting rules to manage these requirements;
- **Cyber or data breaches:** rules on how to manage and report;
- **Records management systems:** Appreciate and recognize different record management and records retention systems;
- **Records Management Policy and strategies:** templates and procedures discussed;
- **Who is responsible for this massive task:** Governance procedures and rules to establish;
- **Implementing the rules:** not a quick term solution... but you will get there by following the guidelines.

# SPECIFIC AREAS UNDER FOCUS

## What is Records Management?

The ISO 15489: 2001 standard defines records management as “the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.”

Records management includes a set of recognized practices related to the life cycle of that information, such as identifying, classifying, archiving, preserving and destroying records.

Some people use the term information governance (IG) when talking about records management. IG is the management of information to support an organization’s present and future, keeping in mind the regulatory, legal, environmental, and operational requirements. It includes the structure, policies, procedures, and processes necessary to manage all the information stored within an organization.

## What is a file plan?

Establishing a file plan is a crucial part of any organisation’s governance strategy. A file plan is a formal inventory of information assets and should be a blueprint for an organisation’s information storage system which in turn will act as a useful tool for risk analysis and information security planning, for identifying critical systems for disaster recovery and business continuity, to inform digital preservation plans and to identify strategic records and information management priorities.

Good infrastructure will ensure your organisational content is secure, findable/searchable and is disposed of at the end of its lifecycle.

## Document security

In a climate of tightening regulations, organisations run an increasingly high risk of non-compliance and unfortunately, non-compliance can have some pretty hefty consequences.

One of every organisation’s top priorities should be to ensure strict data privacy and security measures are in place to safeguard their records and treat client data and information with the security that it deserves.

To ensure that digital and paper files are stored securely, one needs to control who has access to it. When it comes to managing your organisation’s records according to best practices, how and where the documents are stored, is as important as who has access to them.

## Document management practices

POPIA requires the responsible party to “maintain the documentation of all processing operations under its responsibility”. Document mismanagement and lack of an effective record management strategy are key contributors to poor record-keeping and can easily impede an organisation’s compliance to legislative requirements.

A clear and actionable records management strategy should be at the heart of your organisation’s records and information architecture, processes and procedures. It should be based on thorough research of appropriate policies and standards and audited regularly.

## Role of the Information Officer in Records Management

Many organisations are appointing someone in records management as their Information Officer. This shows how important many people consider records management to be in complying with POPIA and the impact that POPIA will have on records management.

## Is a Records Manager a requirement?

In practice, records management usually includes a records manager. This is the person responsible for records management within the organization, but that person often has a team of people working together to create and maintain systems.

Many organisations make a big mistake by underestimating the importance of records management.

According to the ISO 15489-1:2001, records management involves tasks like setting policies and standards, assigning responsibilities and authorities, establishing procedures and guidelines, providing access to management and use of records, and integrating records management into business systems and processes.

## The role of the IT department in Records Management

As technology becomes an increasingly significant aspect of business, records management systems have to keep up. Records management applications (RMAs) are software applications that manage records electronically by using features to categorize and locate active records as well as identify records for disposition. These apps must be secure, reliable, permanent, and comprehensive, and they must comply with rules and regulations. Records management applications simplify the life cycle management of business records without interfering with your organization's line of business.

## Document retention periods

Section 14 of POPIA deals with the retention and restriction of records of personal information, and it prescribes that "records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed". There are however some exceptions, for example where the "retention of the record is required or authorised by law". In some circumstances, you can retain records for "for historical, statistical or research purposes".

Every record has its own lifespan. A records retention program provides for the review, retention and destruction of records received or created in the course of regular business activities.

## Document archiving and legal hold

The need for a legal hold arises out of the duty to preserve information for legal purposes – litigation, government investigation, or audit. The "spoliation of evidence" has become a very costly and time-consuming aspect of many lawsuits, distracting the court's attention from the true merits of a dispute. Having a records retention policy and then issuing a legal hold is becoming a necessary means of doing business.

The 2007 Sedona Commentary described it in two simple sentences: *The duty to preserve information includes an obligation to identify, locate, and maintain, information that is relevant to specific, predictable, and identifiable litigation. When preservation of electronically stored information ("ESI") is required, the duty to preserve supersedes records management policies that would otherwise result in the destruction of ESI. A "legal hold" program defines the processes by which information is identified, preserved, and maintained when it has been determined that a duty to preserve has arisen.* - Sedona Commentary, 2007 Public Comment Version, p.1

- When must a legal hold be established?
- What must be preserved?
- Who is affected? Is it the entire company, or just a division or group of employees?
- Is the legal hold being followed correctly?
- Do I need to expand the reach of the legal hold?
- How long does the legal hold have to remain in effect?
- Are there any implications for the technology resources of the company?

## Document transfers and sharing information in documents

If there is one topic we find ourselves talking about over and over again, it is the need to balance regulatory and compliance requirements with keeping teams and staff operationally effective. Simply put, how can we transform security from a prohibitive exercise into one of enablement? An age old question.

The most recent and best placed example of this, is the GDPR (General Data Protection Regulation). The famous European data protection regulation which requires greater care, control and justification, from data controllers and processors alike, whenever they share or process personal data and documents containing personal data. Practices such as sending personal data in emails with no protection or other insecure communication channels, which was once the norm are now considered too risky.

Refocusing the question on file transfers and file sharing, it becomes how can we continue to share data and documents in an effective manner, yet ensure an acceptable level of security?

## Impact of the National Archives Act on public entities

Archival legislation provides the essential framework that enables a national records and archives service to operate with authority in its dealings with other organs of state.

The legislative provisions in section 13 of the National Archives and Records Service of South Africa Act (Act No 43 of 1996) are aimed towards promoting sound records management and thereby promoting transparency, accountability and better service delivery.

In support of the requirements of the National Archives and Records Service Act, the National Archives and Records Service endorses SANS 15489 Information and documentation – Records management – Part 1: General and Part 2: Guidelines as the required benchmarking tool for records management and, in terms of its statutory mandate, requires governmental bodies to put the necessary infrastructure, policies, strategies, procedures and systems in place to ensure that records in all formats are managed in an integrated manner.

## Drafting a Document Management Policy

At the center of your records management program are your records management policies. These policies define what information your organization must keep as a record, the procedures for managing those records, their retention periods, and procedures for ensuring their secure destruction. They also serve as the organization's institutional memory regarding the establishment of the policies.

## How to implement Record Management Policies and respective responsibility to manage records

The most important component of records management is assigning responsibilities to specific individuals. Tracking who officially approved a particular policy is straightforward, but it's also critical to specify who has long-term responsibility for the various aspects of the policy.



**CCASA members:** R4,485.00\*  
**Non CCASA members:** R6,785.00\*

**Closing date for registrations: 23 September 2021**



The course fee includes the course material in electronic format which will be shared with delegates at least two days before commencement of the workshop. Delegates have an option to request hard copies of the course material at an additional fee of R550.00\*, which includes the courier fee for delivery thereof.

**\*All amounts are inclusive of VAT**

# REGISTRATION FORM

## RECORDS MANAGEMENT COURSE

ONLINE VIA MICROSOFT TEAMS | 30 SEPTEMBER 2021

### DELEGATE'S DETAILS

TITLE:	NAME:	SURNAME:
CONTACT NUMBER:	E-MAIL ADDRESS:	

Are you a member of CCASA?

 Yes No

Do you require hard copies of the course material at an additional fee?

 Yes No

### INVOICING DETAILS

COMPANY NAME:	
POSTAL ADDRESS:	
CONTACT NUMBER:	
VAT REGISTRATION NUMBER:	
PO NUMBER: (IF AVAILABLE)	

### AUTHORISATION DETAILS

NAME OF PERSON AUTHORIZING ATTENDANCE:	
DEPARTMENT:	
CONTACT NUMBER:	E-MAIL ADDRESS:

## TERMS & CONDITIONS:

Registration can only be confirmed once CCASA is in receipt of a completed registration form. Confirmation of registration together with the invoice will be emailed to each delegate. Should you not have received such confirmation within 2 days of sending your registration form, please contact the CCASA offices.

The full fee is payable on presentation of the invoice. The signatories below confirm on behalf of the company that he/she will accept electronic invoices for the purpose of claiming input tax.

CCASA reserves the right to refuse admission where evidence of full payment cannot be shown - please email proof of payment to the CCASA offices as soon as payment has been made.

Registration fee includes course material in electronic format. Hard copies of course material can be bought at an additional fee as indicated on the course outline.

All amounts indicated on the course outline are exclusive of VAT.

In the event of cancellations:

- No refund will be paid for cancellations received in writing less than 4 days before commencement of the course.
- In the event of a cancellation, you are entitled to send a substitute delegate. In this regard, contact CCASA with the changes within 2 days before the event.

CCASA reserves the right to change any part of its published programme due to unforeseen circumstances or reasons beyond our control. CCASA assumes no liability for changes in the programme, date, content, speakers and online platform.

CCASA reserves the right to cancel any event it deems necessary and will in such an event make a full refund of any registration fee. If for any reason CCASA decides to amend or cancel the event we are not responsible for covering any costs incurred by registrants.

Personal data: by providing CCASA with your personal details you give CCASA permission to process such data, which processing will be in line with the CCASA Section 18 Informed Consent notice.

**I / We, the undersigned, have read, understand and agree to the terms and conditions:**

SIGNATURE OF DELEGATE:		DATE:
SIGNATURE OF PERSON AUTHORIZING ATTENDANCE:		DATE:

Send your registration form and duly signed Terms and Conditions to: [admin@ccasa.co.za](mailto:admin@ccasa.co.za)

Enquiries:  
Ronel Lindeque  
e-mail: [admin@ccasa.co.za](mailto:admin@ccasa.co.za) | Tel: (011) 476 3217

**No registration form will be accepted unless the Terms and Conditions have been signed by the delegate and received by CCASA.**