Protection of Personal Information
A 10 step implementation plan

CRS

Rivonia

Paul Mullon
0832736087
paulm@corconcepts.co.za

29 October 2015

Agenda

- POPI in context
- POPI and Information Governance (IG)
- A 10 step POPI Implementation plan
- Questions and discussion

POPI Summary

Refresh: Information must be:

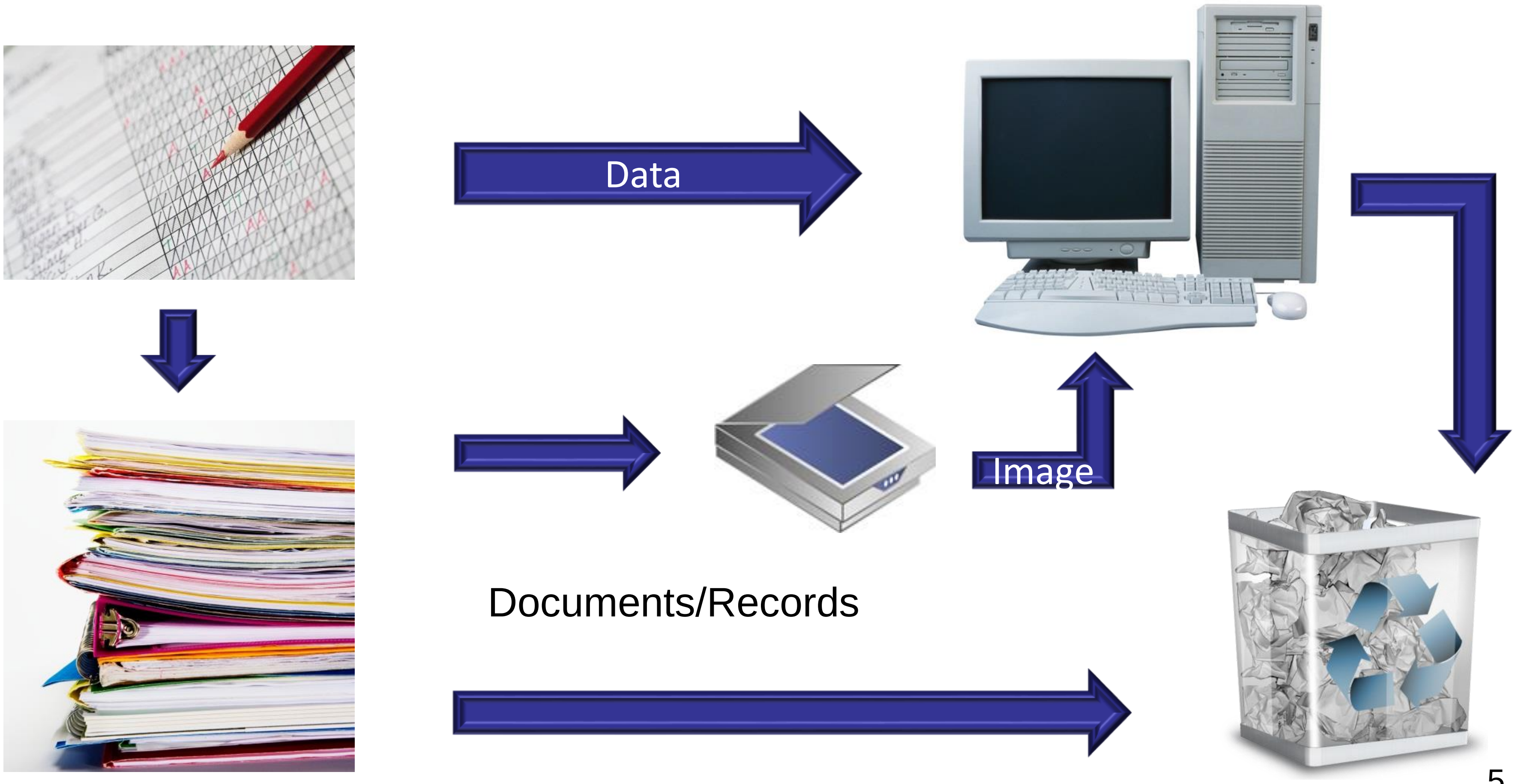
- obtained fairly and lawfully;
- used only for the specified purpose for which it was originally obtained;
- adequate, relevant and not excessive to purpose;
- accurate and up to date;
- accessible to the subject;
- kept secure;
- destroyed after its purpose is completed.

Forms of information and POPIA considerations

- All content regarding the individual must be identifiable
- Information must be deleted once the purpose for which it was gathered is over
- The client must be informed why the information is being captured, and how it will be used.

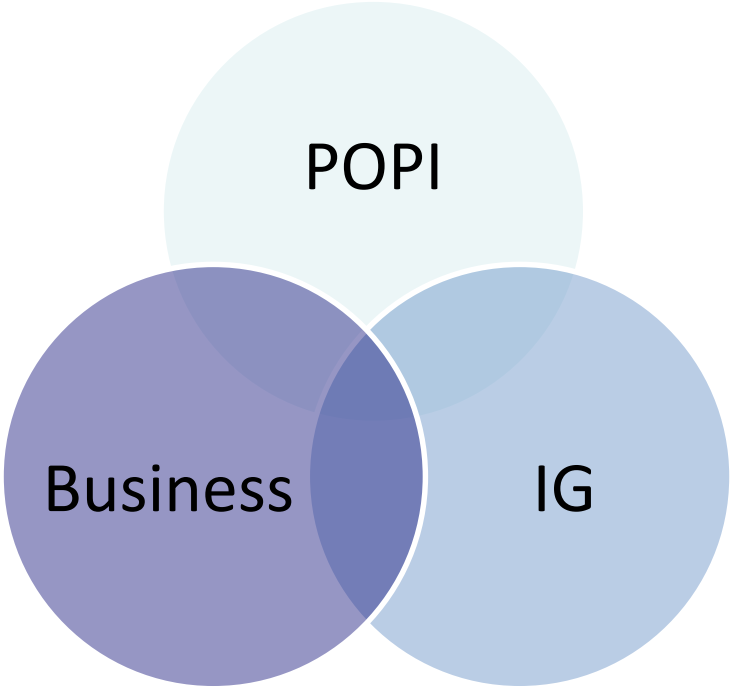
Forms of information POPIA considerations

Protection of Personal Information – all must be managed consistently



POPI and IG

POPI, the Business and Information Governance are inseparable

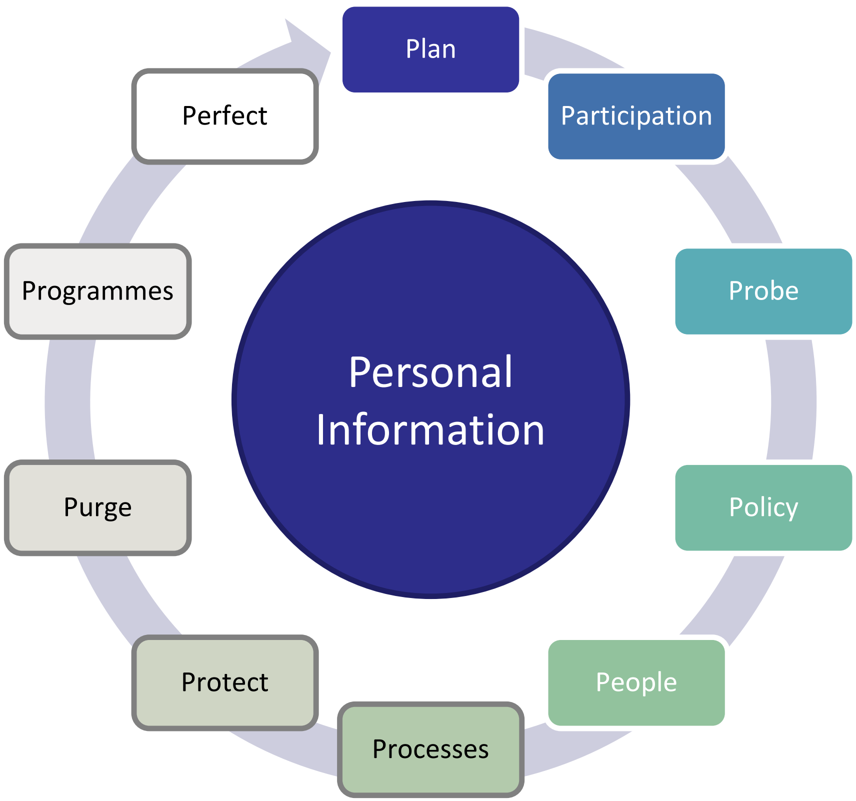


Formats for Personal Information & Information Governance

- Data Governance
  - POPI information will be in databases and systems
- Born digital documents
  - Should they be printed?
  - Legal principles, integrity, authenticity and admissibility
  - The role of signatures
- Conversion of paper to electronic
  - When to scan
  - What to scan
  - Scan and destroy
  - The use of e-forms for data capture

Personal Information (PI) + IG Actions

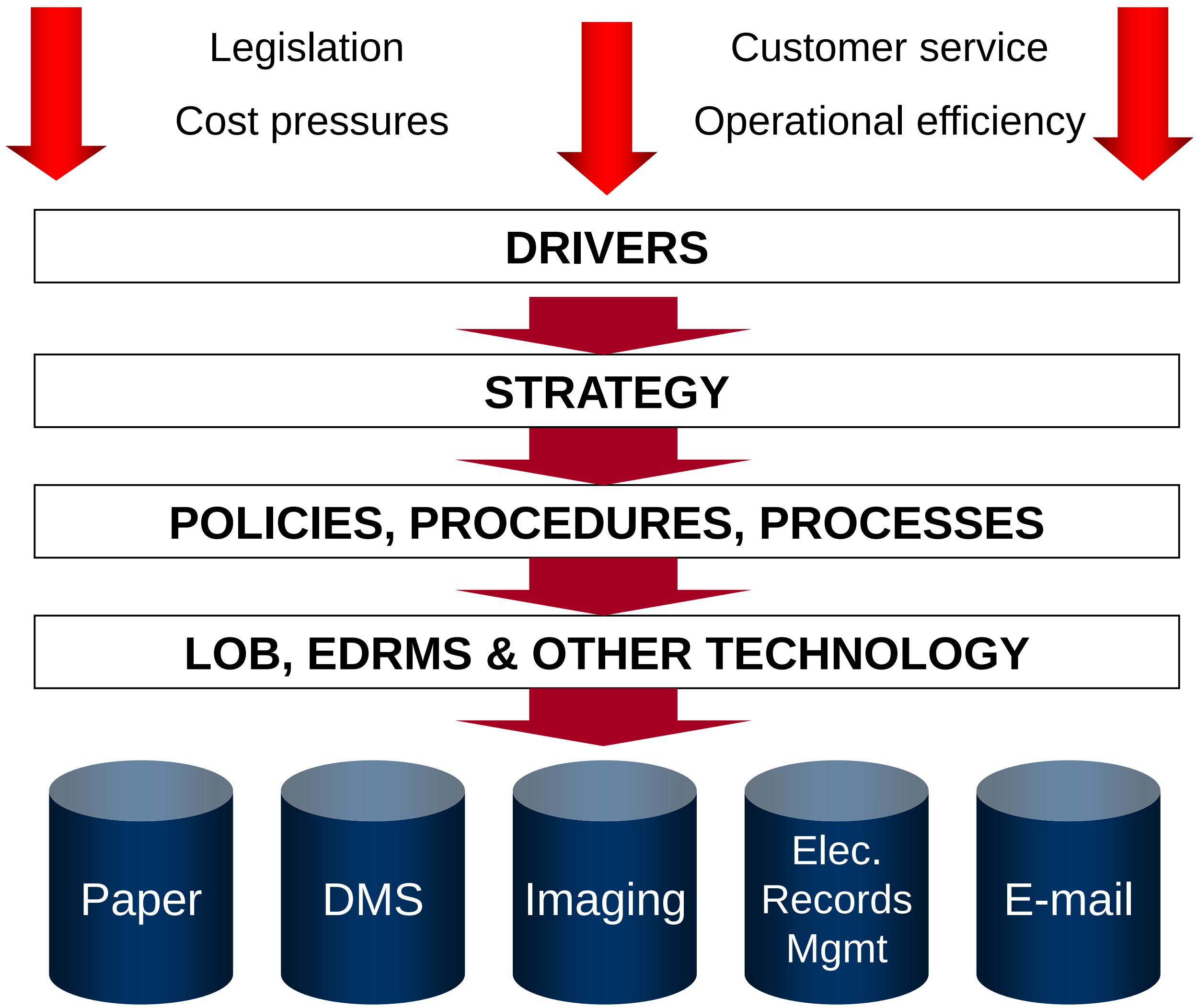
Consolidated view



The 10Ps of PI

1. Plan
2. Participation (+Governance) structures)
3. Probe (understand your information)
4. Policy (+Procedures & Practices)
5. People (Educated and aware)
6. Processes
7. Protect
8. Purge
9. Programmes (Systems)
10. Perfect

Plan: The process



Participation: Governance and Control

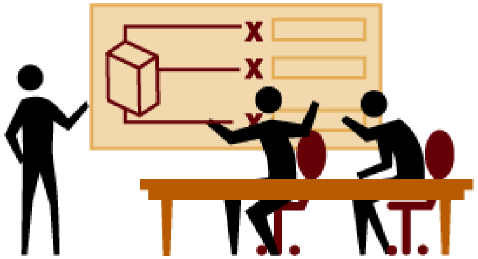
Steering Committee

Multi-Disciplinary

- IT
- Operational Divisions
- Group Support Services
- Legal
- Compliance
- Risk
- Records Management

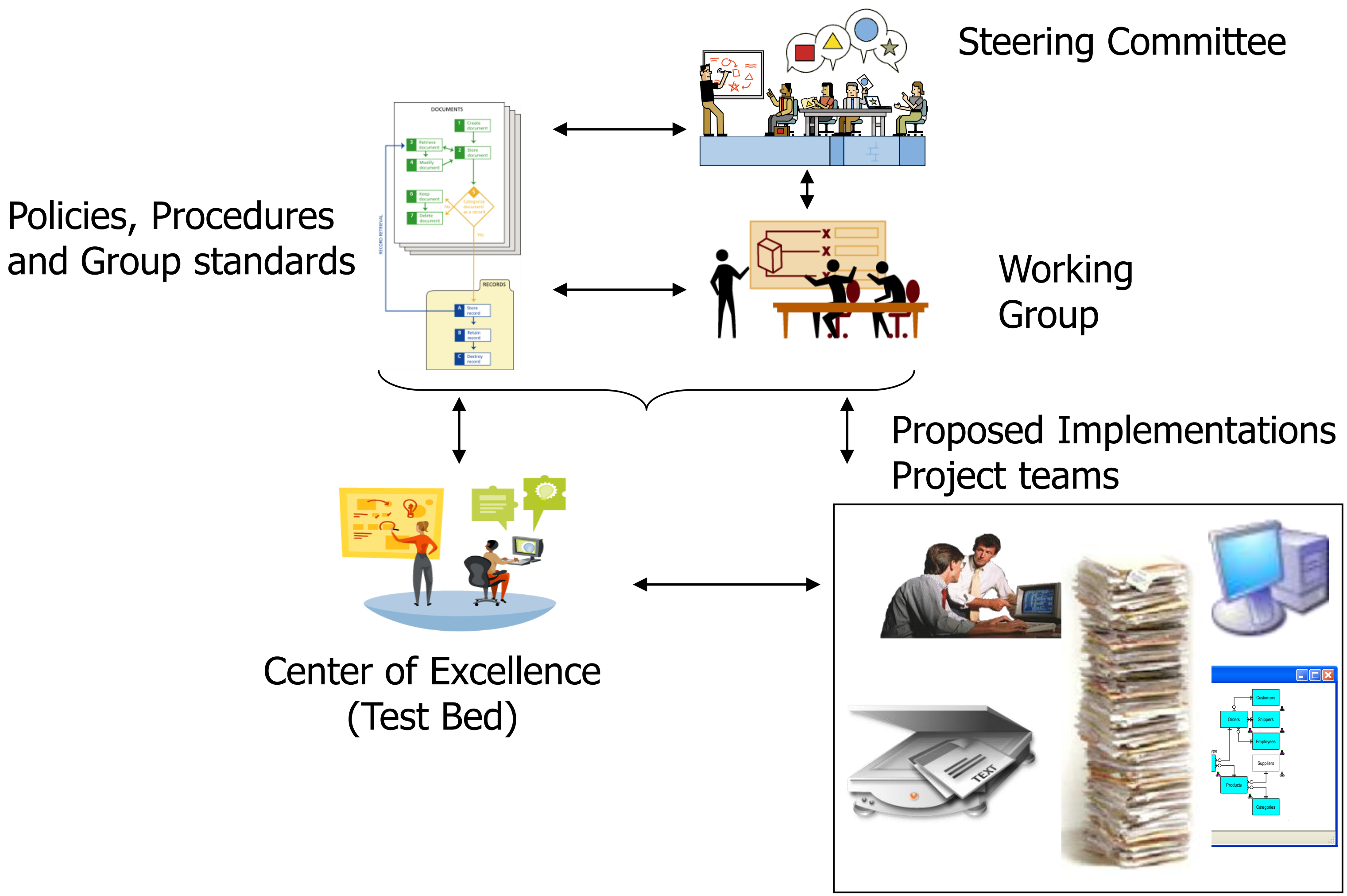
Working Groups

- IT
- Operational Divisions
- Group Support Services
- Records Management



The purpose of these teams are to ensure that the necessary governance instruments are in place, maintained, reviewed, & refined as appropriate.

Governance Inter-relationships



Probe – understanding your information

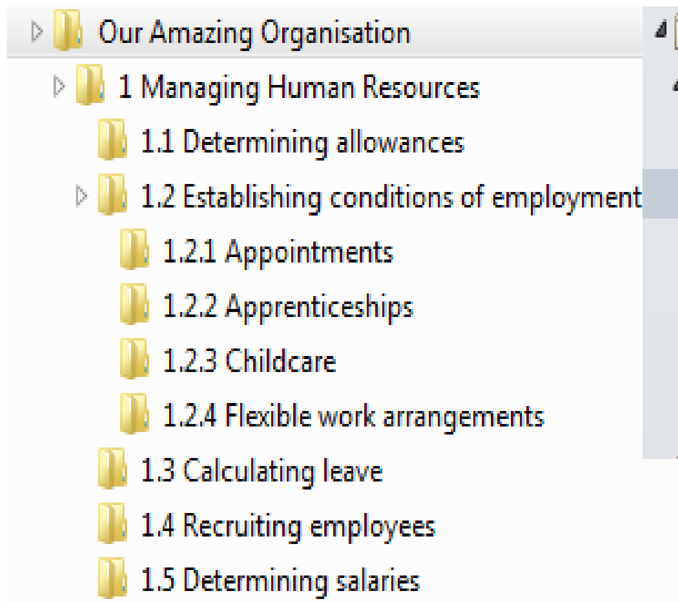
Reference	Description	Retention period	Retention trigger	Personal Information?
Originating process	Other processes	Formats – Paper, electronic, data	Scan and destroy	Sensitivity classification
Index fields	Naming convention	Custodian Stewards	Owner	Applicable legislation
Which systems	Business Units	Extracted to other systems	Summarised in reports	…

Integrated classification systems

Paper classification

1. Managing Human Resources
1.1 Determining Allowances
1.2 Establishing Conditions of Employment
 1.2.1 Appointments
 1.2.2 Apprenticeships
 1.2.3 Childcare
 1.2.4 Flexible work arrangements
1.3 Calculating Leave
 1.3.1 Accrual
 1.3.2 Entitlements
 1.3.3 Holidays
 1.4 Recruiting Employees
 1.5 Determining Salaries
 1.5.1 Deductions
 1.5.2 Overtime
 1.5.3 Remuneration
 1.5.4 Superannuation

Electronic classification



E-mail classification

Don’t ignore metadata
Build business rules into systems

Policy

- Policies + Procedures +Processes +Practices
- Integrated policy framework
- Enforceable, monitored, enforced

At some stage we have to trust people

Be prepared to monitor

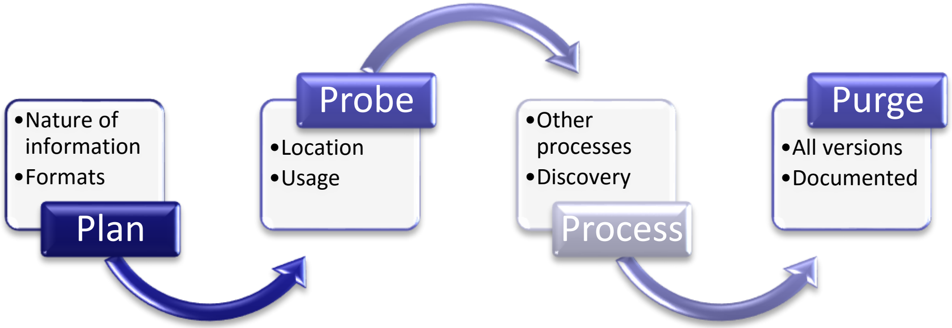
Be prepared to enforce

People

- Implement a change management programme
- Awareness and training are key
  - All people who manage content
  - Administrators
  - Process owners
- Build compliance into KPIs.

Processes

- POPI and IG are business issues
- A multi-disciplinary approach is needed
- Be practical
- Look for process integration and improvement opportunities
- Understand which PI is used in which processes
- POPI is not a separate process



Protect: Information Security

- Kept secure (in all formats)
- Physical and digital security
- Encryption
- Removable media
- Confidential destruction
- Kept complete
- Discoverable
- Records Holds
- Audit trails

Purge

- An opportunity to:
  - Conduct data cleansing and normalisation
  - Identify and improve redundant processes or steps
  - Remove the rubbish:
    - duplicates
    - “non-records”
    - past-due records

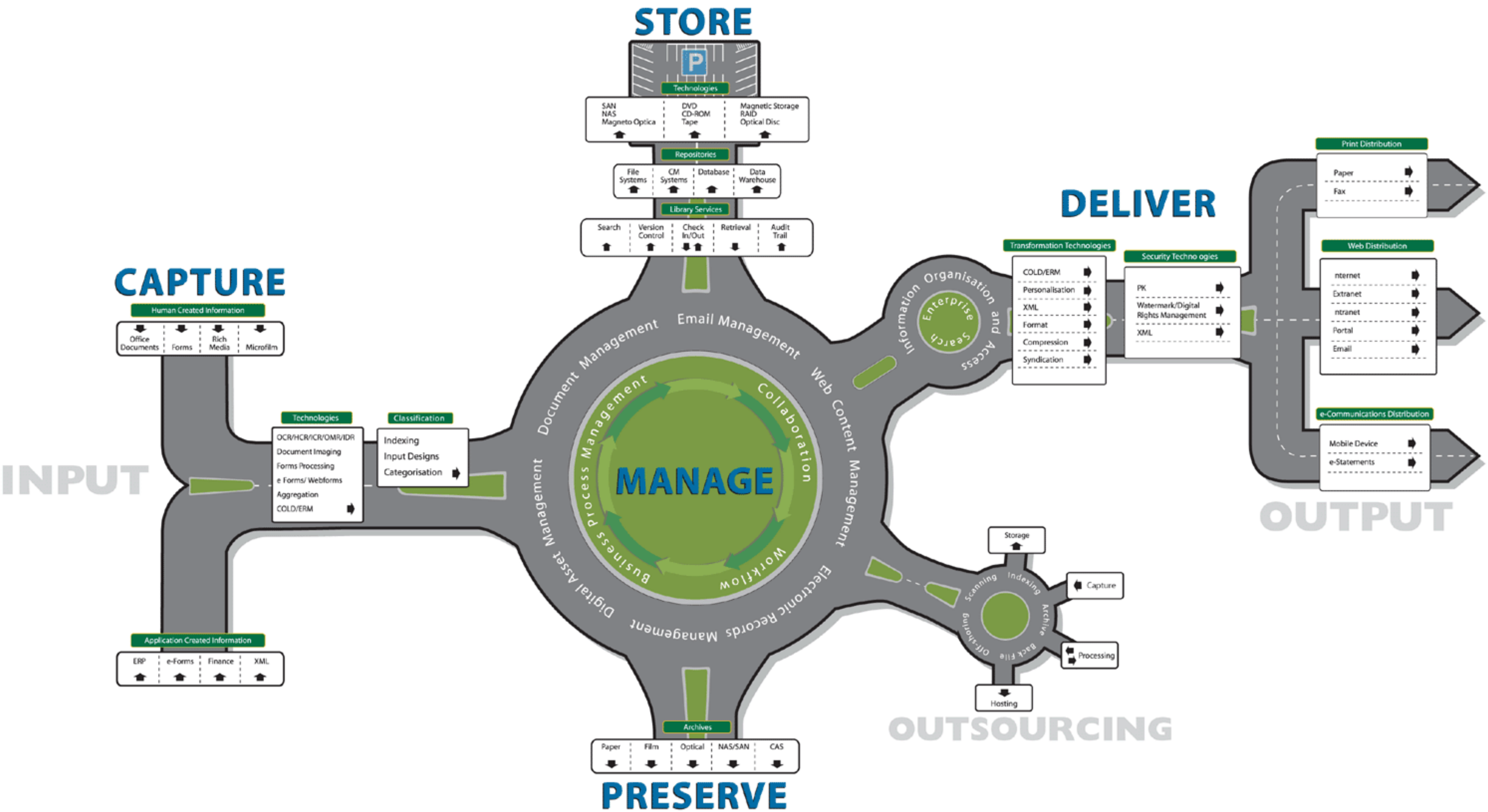
Programme:

Take a Programme Management approach

- POPI is a programme
- You’re in it, and will be for the long term
- Treat each initiative as a project
- You won’t be totally compliant from day one.

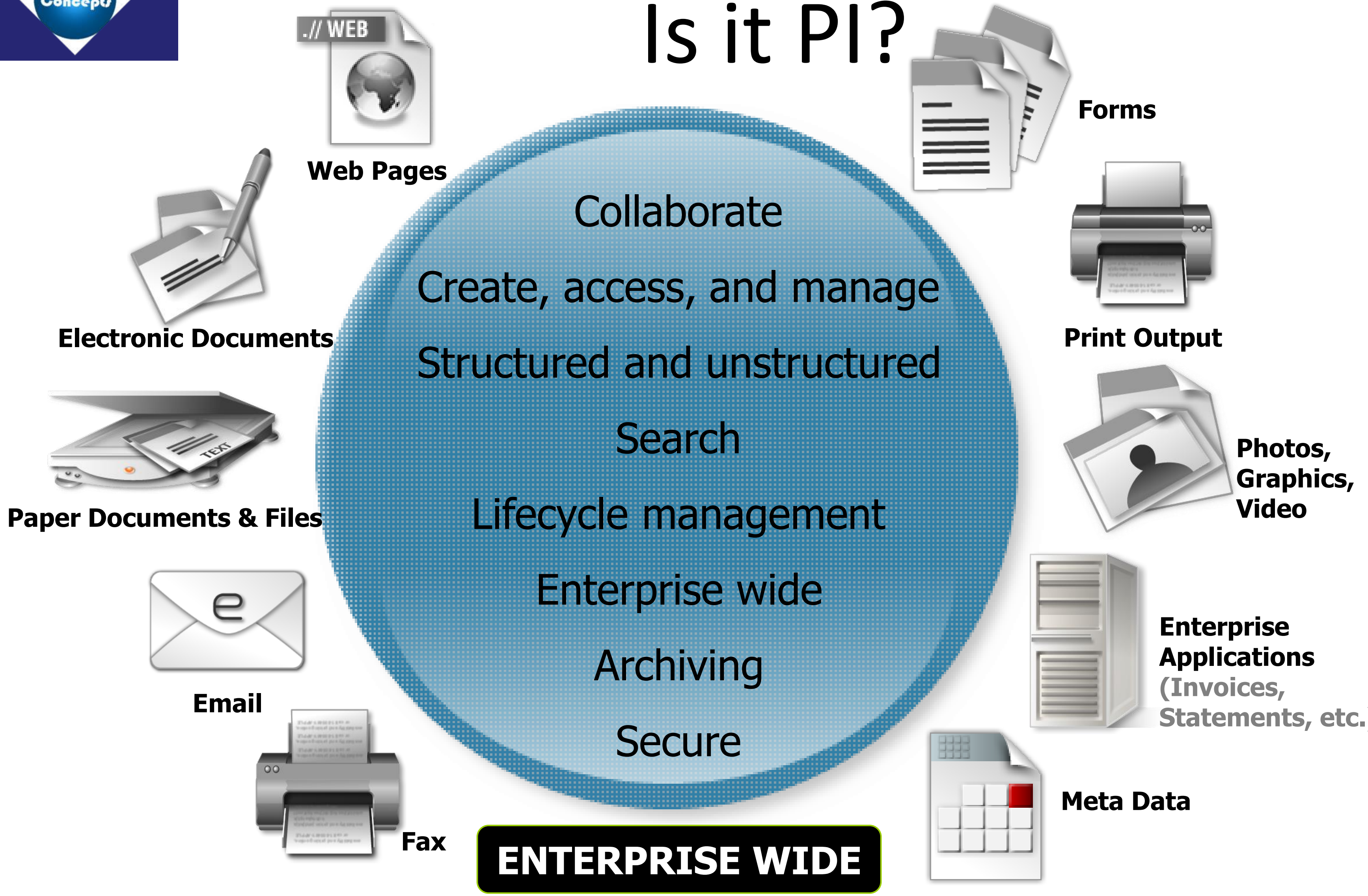
Programmes:

Enterprise Content Management (ECM)



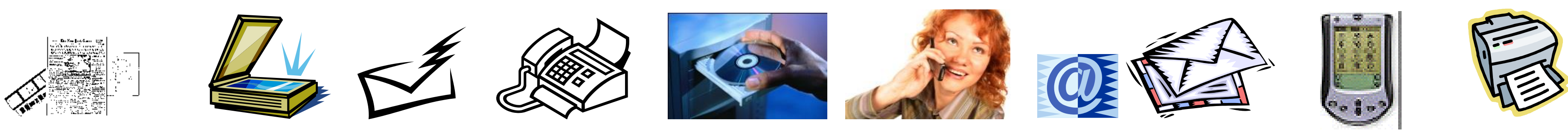
Source: AIIM

What is Content? Is it PI?



Processes
Flows of information

Internally or externally generated



Value determination

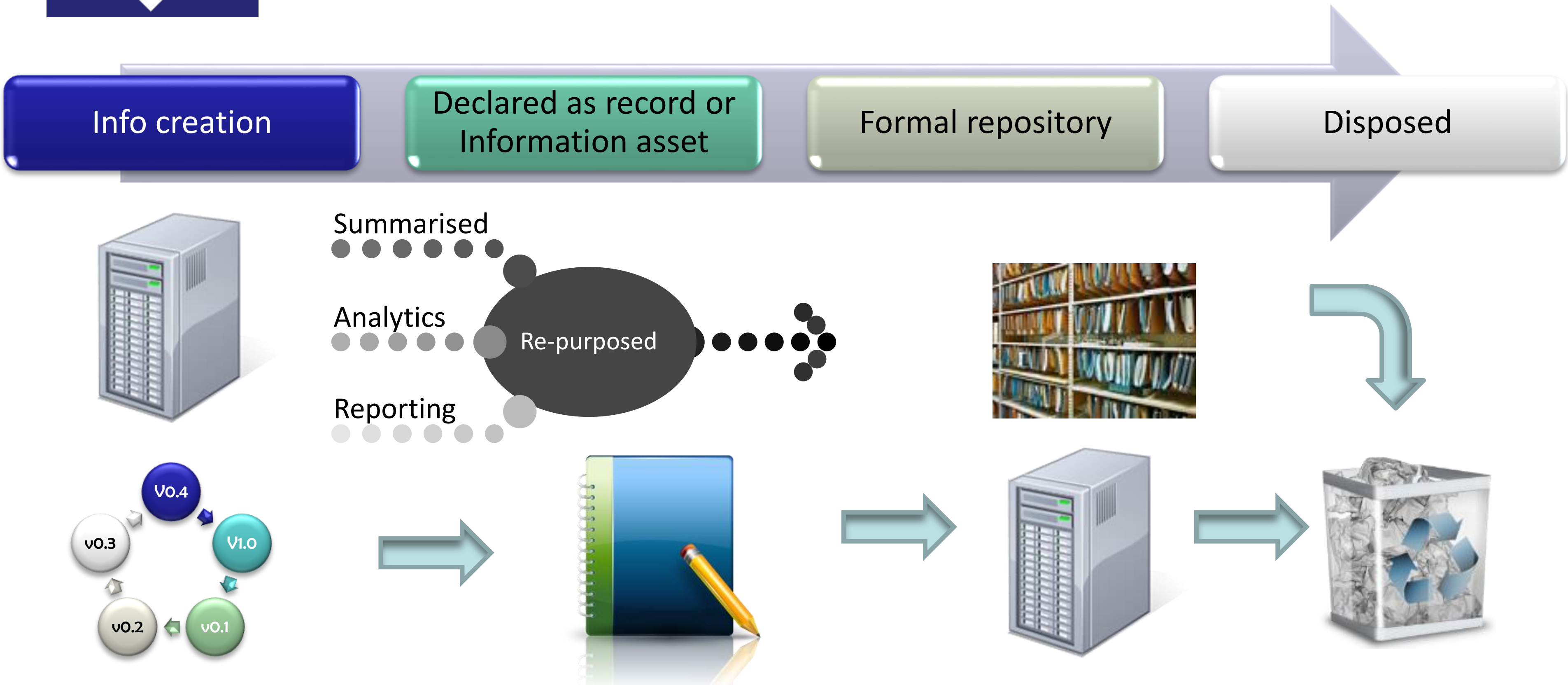
Is it a record, or a document, is it PI or all of the above?

Why must it be kept?

What must be kept?

Who must keep it?

Information processes

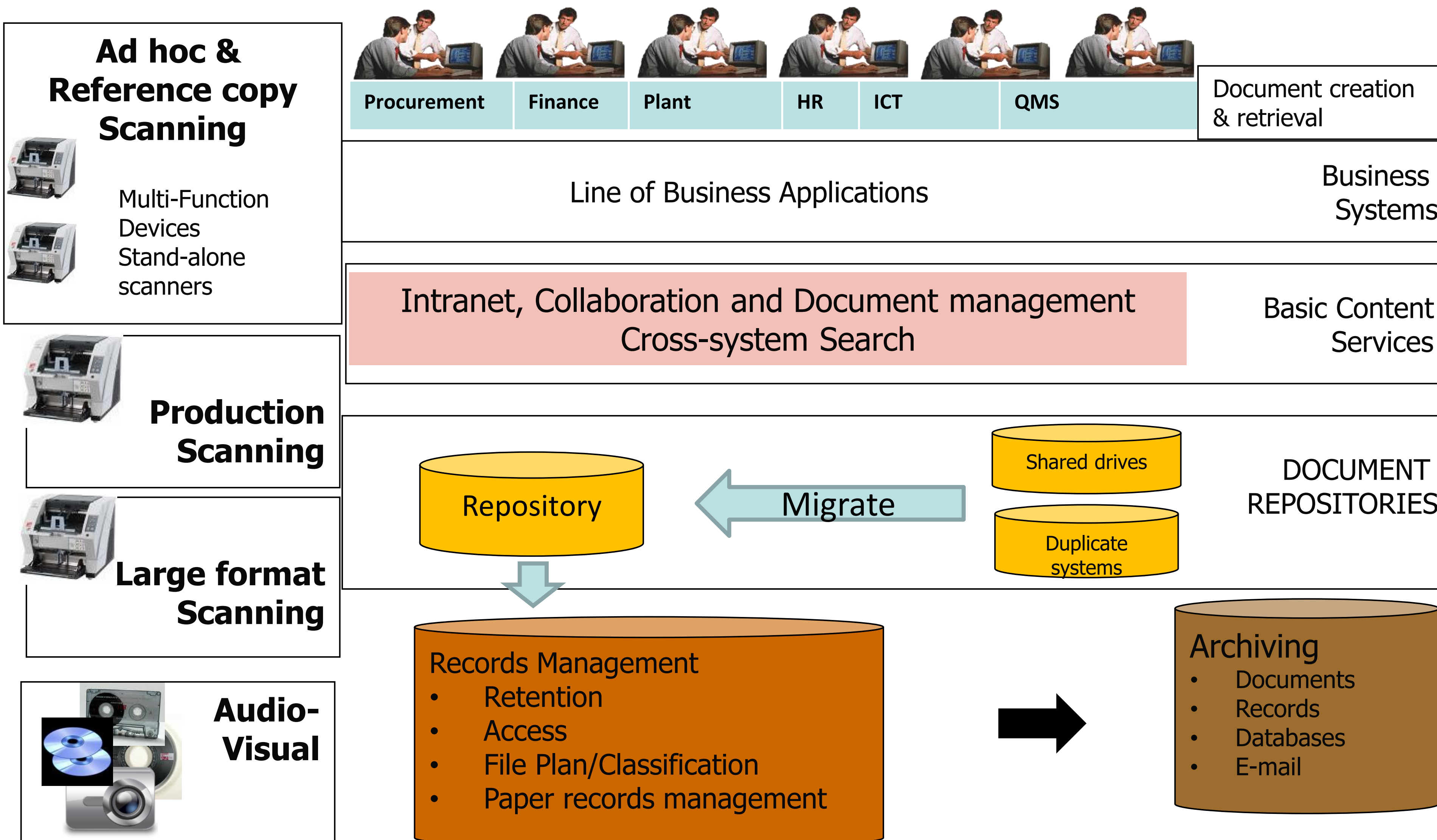


Who creates or receives it
What format is it in?
Should it be converted?
Where is it?
Where can it be stored?
Which processes require it?

What rules are in place?
Who creates them?
How are they implemented in systems?
What intervention must users take?

Where must they be stored?
When?
How?
By whom?

Programmes: Architecture



IG – What is it?

- the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals

IG Is broader than POPI
IG Spans multiple domains

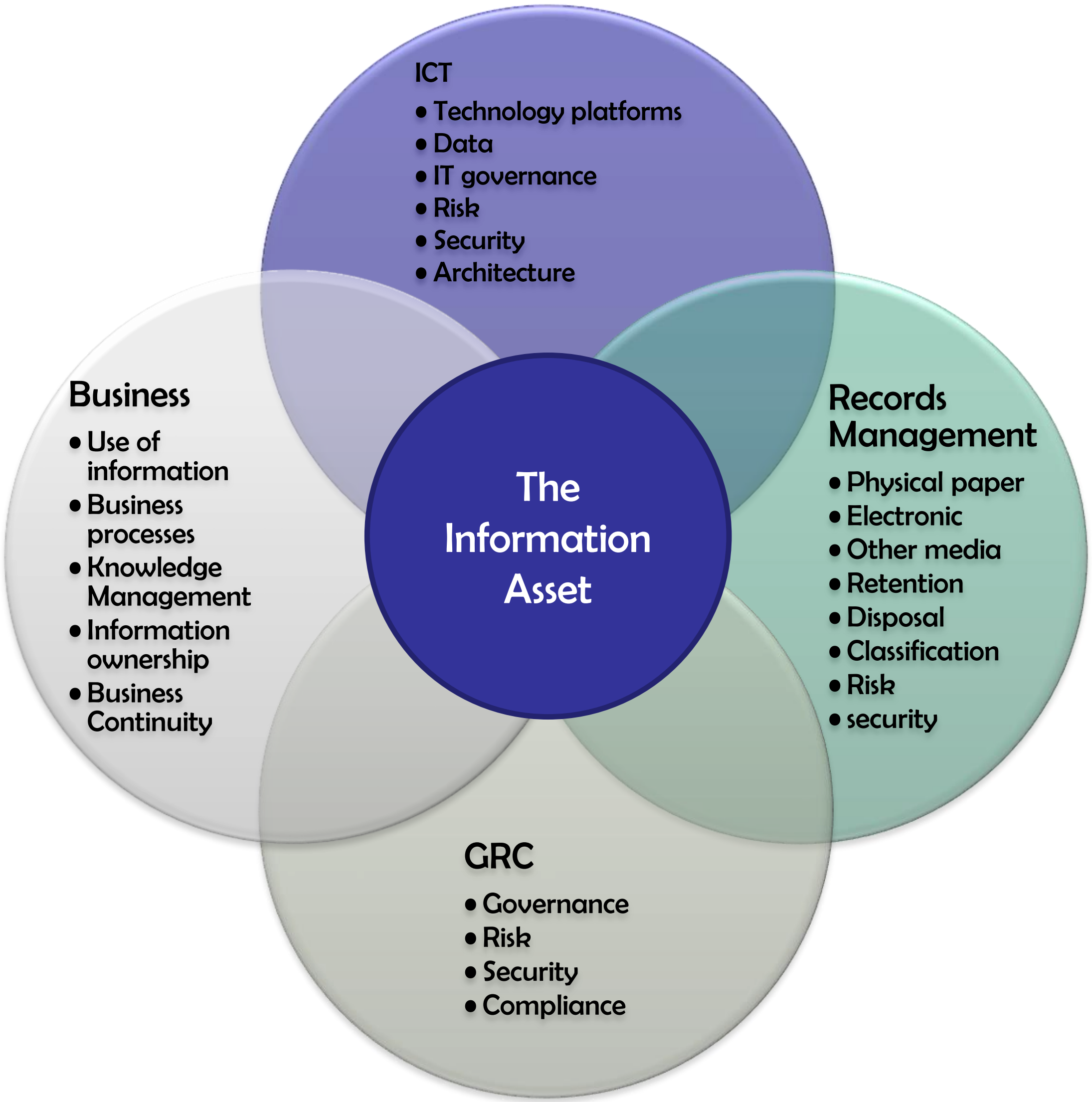
Gartner

Typical drivers/domains

- Corporate Governance (King III)
- Data Privacy (POPI)
- Other legislation (FICA, Companies Act, ECT)
- Information security
- IT Governance
- Records Management
- Master Data Management (Governance & quality)
- Quality (ISO 9001 and SHEQ)

Domain overlaps

- Information is a Business Asset
- ICT provide platforms
- Records Management provides custody
- GRC Provides Governance
- PI Spans all…



Integrated Information Governance

Key Success Factors

- Executive Buy-In
- Aligned to Corporate Goals
- Integrated approach
- Change Management
- Stakeholder inclusion

Common Features

- Governance Structures
- Strategy
- Policies
- Procedures
- Standards
- Metrics
- Reviews
- Benchmarked

Principles

- Accountability
- Integrity
- Protection
- Compliance
- Retention
- Disposition
- Transparency
- Availability

Domains

- Corporate Governance
- Records Management
- IT Governance
- Data Privacy
- Knowledge Management
- Master Data Management
- Information Security
- Information Risk

Information life cycle

Principles (GARP)

(Generally Accepted Recordkeeping Principles)

Principle of Accountability

- An organization shall assign a senior executive who will oversee the program and delegate program responsibility to appropriate individuals, adopt policies and procedures to guide personnel, and ensure program auditability.

Principle of Integrity

- A program shall be constructed so the records and information generated or managed by or for the organization have a reasonable and suitable guarantee of authenticity and reliability.

The GARP Principles

Principle of Protection

- A program shall be constructed to ensure a reasonable level of protection to records and information that are private, confidential, privileged, secret, or essential to business continuity.

Principle of Compliance

- The program shall be constructed to comply with applicable laws and other binding authorities, as well as the organization's policies.

The GARP Principles

Principle of Availability

- An organization shall maintain information in a manner that ensures timely, efficient, and accurate retrieval of needed information.

Principle of Retention

- An organization shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational, and historical requirements.

The GARP Principles

Principle of Disposition

- An organization shall provide secure and appropriate disposition for records and information that are no longer required to be maintained by applicable laws and the organization's policies.

Principle of Transparency

- The processes and activities of an organization's program shall be documented in an understandable manner and be available to all personnel and appropriate interested parties.

Accountability

- The senior executive in charge should establish a method to design and implement a structure to support the program.
- Governance structure should be established for program development and implementation.
- Necessary components include an accountable person and a developed program.
- The program should have documented and approved policies and procedures to guide its implementation.
- Auditability enables the program to validate its mission and be updated as appropriate.

Integrity

- Correctness of and adherence to the policies and procedures of the organization
- Reliability of the information management training and direction given to the employees who interact with all systems
- Reliability of the records and information created
- An acceptable audit trail
- Reliability of the systems that control the recordkeeping including hardware, network infrastructure, and software

Protection

- Information audit determines the records and information and the required protection
- Implementation of appropriate controls throughout the lifecycle
- Systems to have adequate controls
- Physical and system controls
- Vetting of staff
- E-mail and removable media controls
- Implementing sensitivity classification

Compliance

1. The system must contain information (and audit trails) showing that the organization's activities are conducted in a lawful manner.
2. The system is itself subject to legal requirements such as requirements to maintain tax or other records and information.
   – Know what information must be entered into its records to demonstrate that its activities are being conducted in a lawful manner
   – Enter that information into its records in the manner prescribed by law
   – Maintain its records in the manner and for the time prescribed by law

Availability

Organizations must have the ability to identify, locate, and retrieve the records and related information required to support its ongoing business activities. These records are used by:

- Individuals and groups to reference, share, and support their work
- Legal and compliance for discovery and regulatory review purposes
- Numerous corporate functions to validate management decisions and account for the resources of the organization.

Retention

Implement Retention periods including requirements for:

- Legal and regulatory
- Fiscal
- Operational
- Historical

Disposition

- At the completion of the retention period for an organization's records, the records must be designated for disposition.
- Transfer or destruction
- Implement records holds
- Formal approval and documentation of all disposition activities

Transparency

Records documenting the programme must:

- Document the principles and processes that govern the programme
- Accurately and completely record the activities undertaken to implement the programme
- Be written or recorded in a manner that clearly sets forth the information recorded
- Be readily available to legitimately interested parties

Conclusion: Benefiting from POPI +IG

- Don’t treat it as a compliance initiative
- Seek benefits from understanding your information and revising processes
- Use it as a catalyst to implement sound Information Governance
- Information Governance is a programme, a journey.

Questions?

Questions and further discussion

Paul Mullon
0832736087
paulm@corconcepts.co.za