Protection of Personal Information
A 10 step implementation plan

Paul Mullon
0832736087
paulm@corconcepts.co.za

Agenda

- POPIA in context
- Provisions of the Act
- Information formats
- A 10 step POPIA Implementation plan
- Questions and discussion

Status of POPIA

Signed into law in November 2013

- Certain sections came into force on 11 April 2014
  - Section 1 – contains the definitions and sets out the purpose of POPIA
  - Part A of Chapter 5 which provides for the establishment of the Information Regulator
  - Other Sections which allow for the making of regulations where they are required in the Act.
- Information Regulator appointed 1 December 2016 for 5 years
- Regulator gives right to Privacy as enshrined in the Constitution
- 1 year to comply once regulations are in place (May be extended to 3 years)

Information Regulator

Information Regulator

PAIA

Freedom of Information

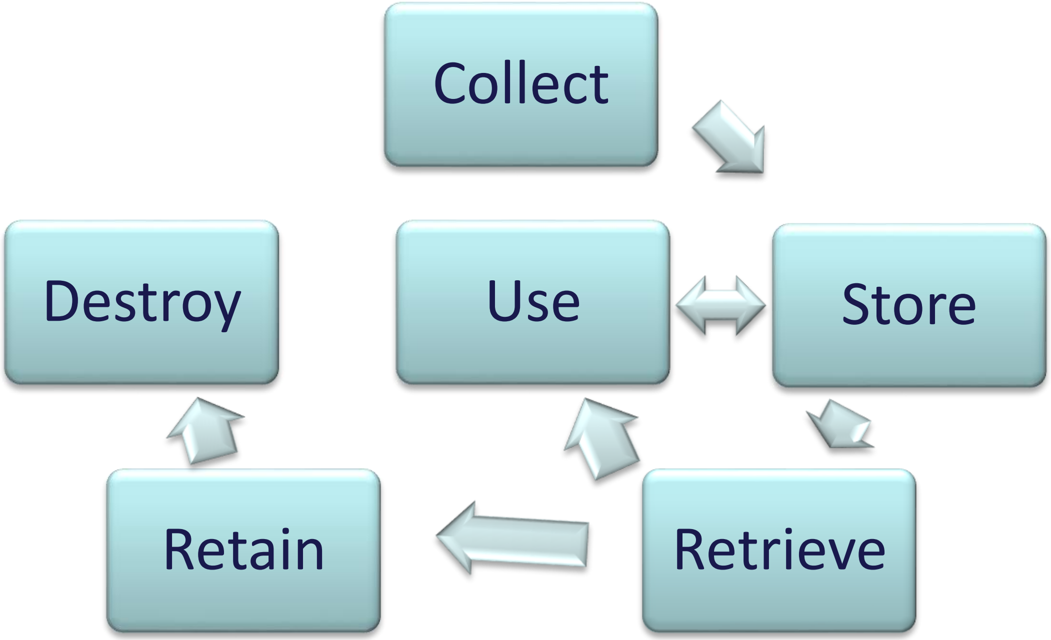
POPIA

Privacy

Purpose

Gives effect to the right to Privacy

To regulate the processing of personal information by public and private bodies



POPIA Summary

Summary: 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.

Provisions

- Protection of personal information processed by public and private bodies
- Conditions establishing minimum requirements for processing of personal information
- Establishes an information Regulator

Provisions

- Provides rights regarding unsolicited electronic communications and automated decision-making i.e. direct marketing
- Regulates flow of personal information across borders of the Republic i.e. cloud servers

Personal Information

Information about:

- An identifiable, living, natural person's information, and where applicable, an identifiable, existing juristic person's information, including:
  - Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person
  - Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person

Personal Information

- The name of the person if it appears with other personal information related to the person or if the disclosure of the name itself would reveal information about the person
- The biometric information of the person, fingerprint, blood, retina scan
- The personal opinions, views or preferences of the person
- The views or opinions of another individual about the person

Rights of Data Subject

The right to have personal information lawfully processed, including:

- Notification
  - Collection
  - Accessed or acquired
- Ability to object
- Establishing whether the responsible party holds information
- Request correction, destruction or deletion

Rights of Data Subject

Application provisions

- Refuse processing for direct marketing by unsolicited electronic communications
- Complaint Regulator
- Institute civil proceedings

Exclusions

Does not apply to:

- Processing in the course of purely personal or household activity
- De-identified and cannot be re-identified
- By a public body regarding national security or prevention and detection of criminal activity
- Research and statistical purposes

Exclusions

- Prosecution of offenders (proceeds of unlawful activities)
- Execution of sentences or security measures
- For Exclusively Journalistic Purposes
- By the Cabinet and Committees and Executive Council
- Relating to judicial functions of the court

8 Conditions for Lawful Processing

1. Accountability – who is responsible for safeguarding information
2. Processing Limitations – must justify reason
3. Purpose specification – must justify purpose
4. Further Processing limitation – required in future

Conditions of Lawful Processing

5. Quality of Information – complete, accurate, not misleading, & updated
6. Openness
7. Security Safeguards – physical and electronic
8. Data Subject Participation

Accountability

The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with <u>at the time of the determination of the purpose</u> and <u>means of the processing</u> and <u>during the processing</u> itself.

Conditions for Lawful Processing

- Processing Limitations
  - Data subject to consent – written, specific and voluntary
  - Processing necessary to carry out actions to conclude or perform a contract to which the data subject is a party e.g. delivery address
  - Processing compliance with an obligation imposed by law or acting in public interest
  - To protect the legitimate interest of data subject

Conditions for Lawful Processing

Processing Limitations:

- For proper performance of public law duty by a public body
- Pursue legitimate interests or of other responsible party or third party to whom the information was supplied
- Data subject may withdraw consent
- Data subject may object on reasonable grounds

Conditions for Lawful Processing

Purpose Specific

- May not retain records in no longer necessary
- Must destroy records if no longer authorized to retain

Further Processing

- Original Purpose
- Consent required

Conditions for Lawful Processing

Information Quality

- Complete, accurate and up to date

Openness

- Notify when collecting

Security Safeguards

- Integrity and confidentiality
- Notify data subject and Regulator of breach

Offences & Penalties

- Various Offences – may start with enforcement notice
- Minor Offences:
  - Fine and/or imprisonment up to 12 months
- Major Offences:
- Fine and/or imprisonment up to 10 years

Enforcement

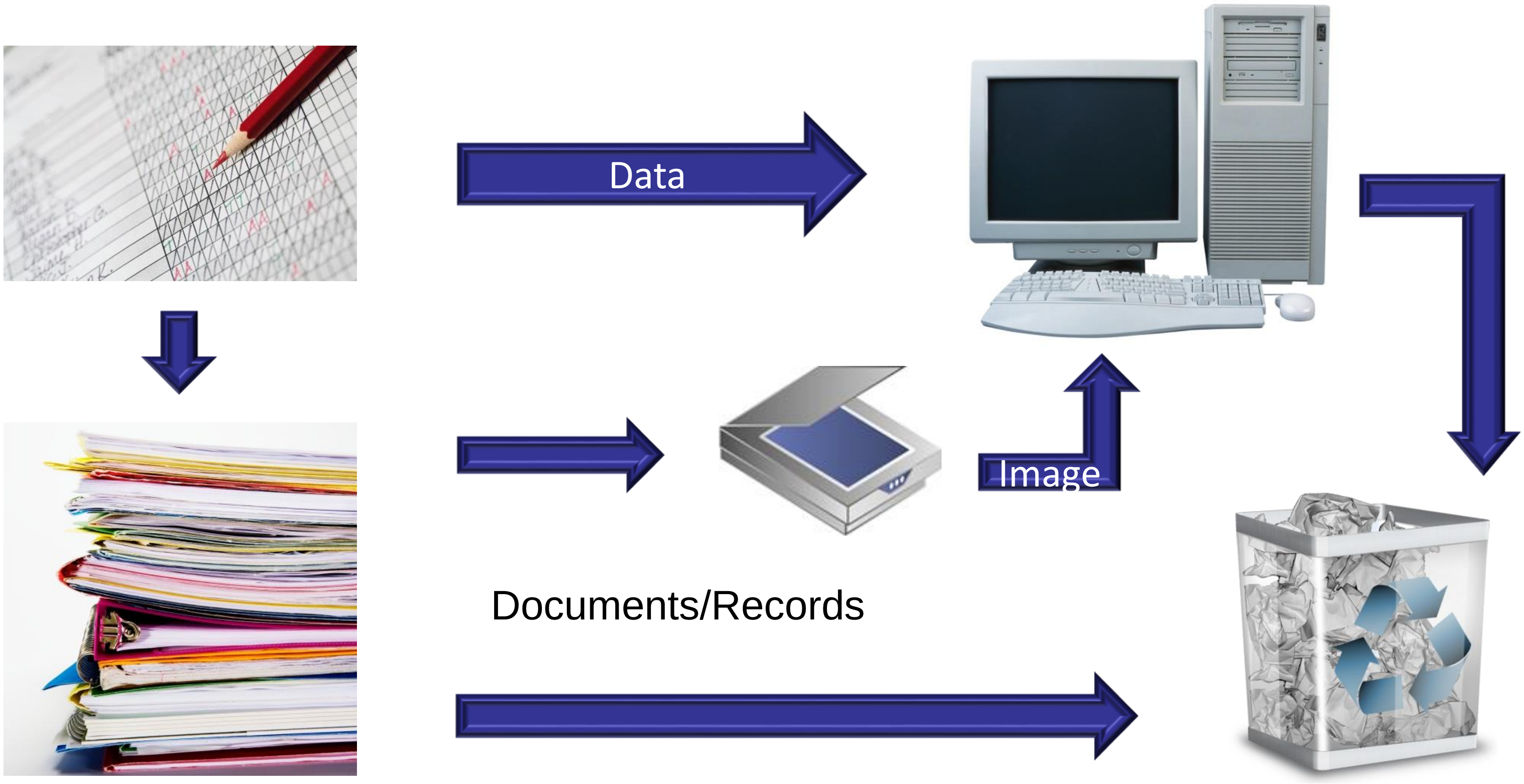
- Regulator may:
  - Monitor and enforce complaints
  - Settle
  - Serve information notice
  - Administrative fines (R10 Million)
- Civil Proceedings:
  - Regardless of intention or negligence
  - Damages patrimonial and non-patrimonial
  - Aggravated damages
  - Interest costs

Forms of information and POPIAA 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 POPIAA considerations

Protection of Personal Information – all must be managed consistently

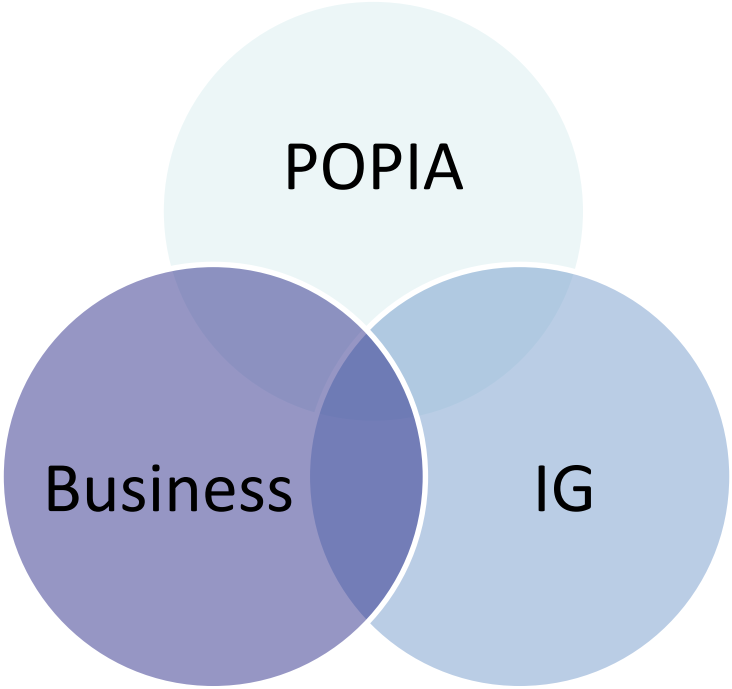


Formats for Personal Information

- Data Governance
  - POPIA 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

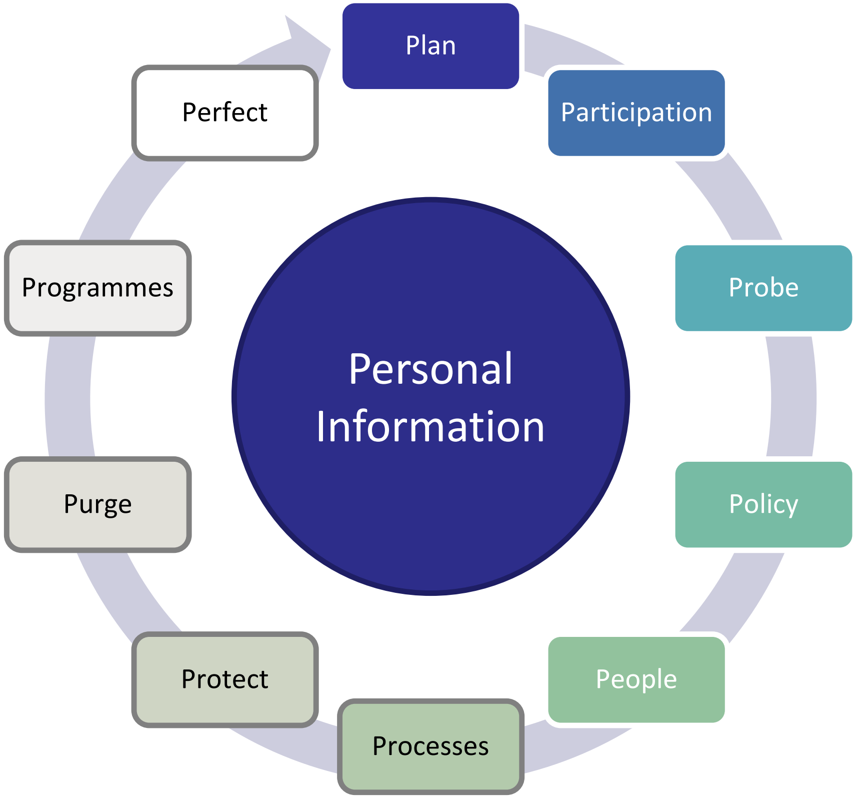
POPIA and IG

POPIA, the Business and Information Governance are inseparable



Personal Information (PI) Actions

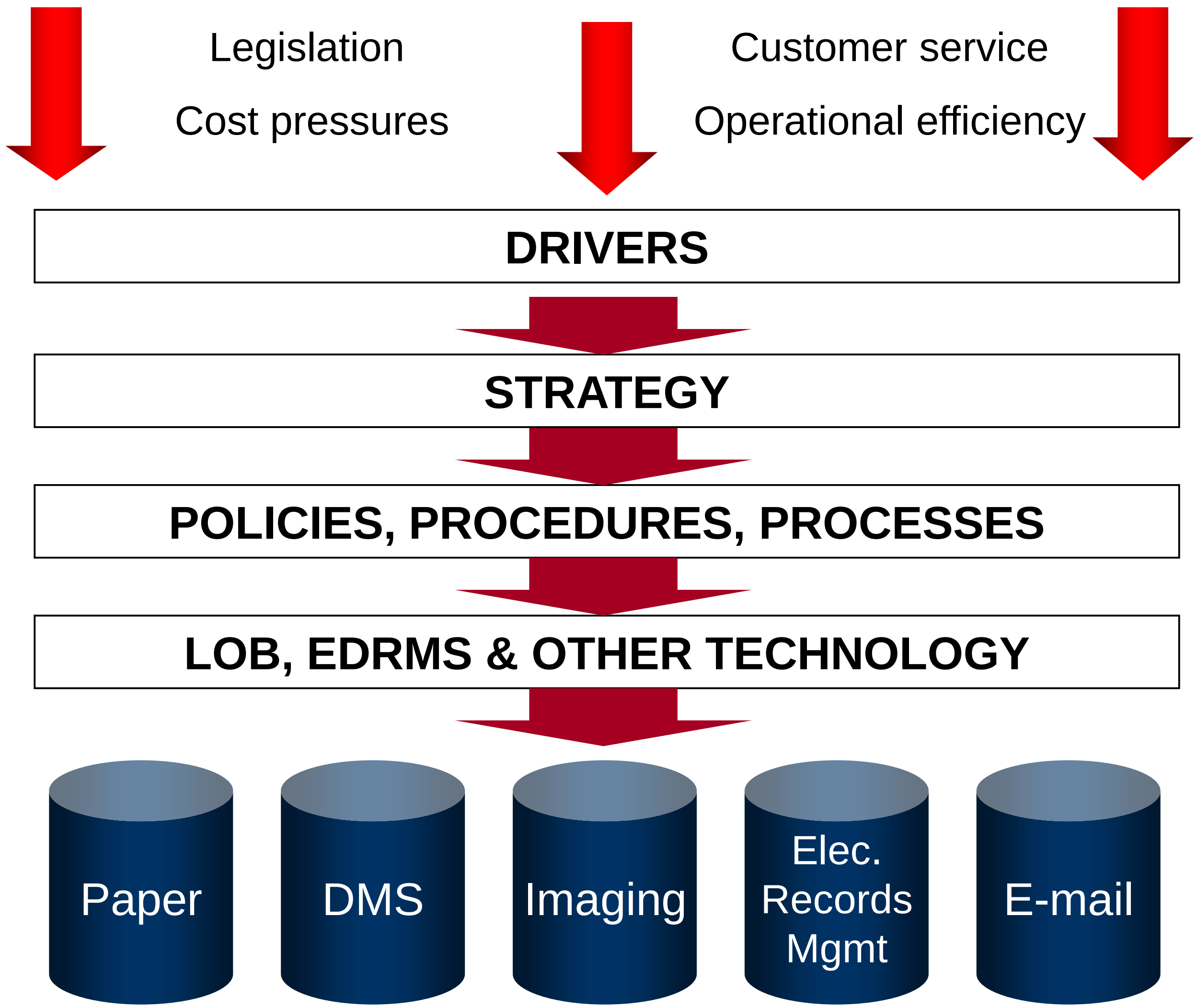
Consolidated view



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



Plan

- Adopt an 80:20 philosophy
- Address the burning issues first
    1. Client and prospect information
    2. Human Resource information
    3. Supplier information
- Treat it as a programme with discrete projects
- Allocate resources

Plan

- Employ change management techniques
- Management commitment throughout
- Build compliance into day-to-day processes

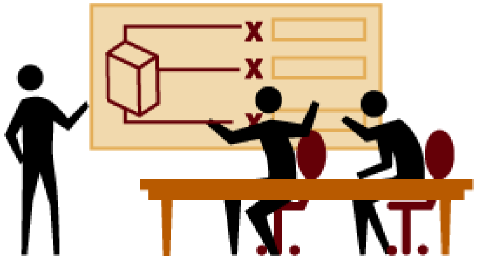
Participation: Governance and Control

Steering Committee

Multi-Disciplinary

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

Working Groups

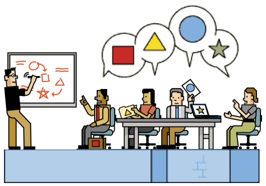


- IT
- Operational Divisions
- Group Support Services
- Records Management

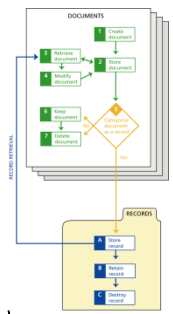
The purpose of these teams are to ensure that the necessary governance instruments are in place, maintained, reviewed, & refined as appropriate.

Governance Inter-relationships

Steering Committee



Policies, Procedures
and Group standards



Working
Group

Center of Excellence
(Test Bed)

Proposed Implementations
Project teams

Multiple inputs

- Sales
- Marketing
- IT
- Records Management
- Legal
- HR

Probe – understanding your information

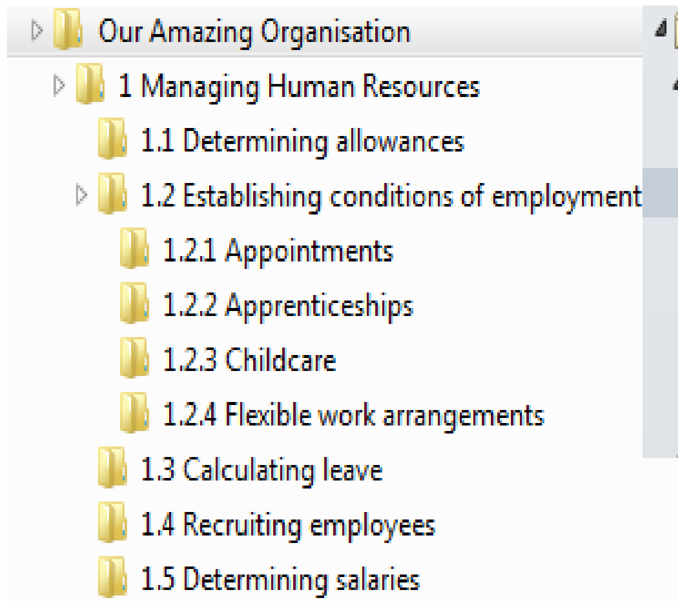
Reference	Description	Retention period	Retention trigger	Personal Information?
Originating process	Other processes	Formats – Paper, electronic, data	Scan and destroy	Sensitivity classification
Index fields	Naming convention	Custodian Stewards	Owner	Applicable legislation
Which systems	Business Units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

Review related policies

- PAIA
- Human Resources
  - Conditions of employment
  - Verification
  - Selection
- Records Management
- ICT
- Information security

People

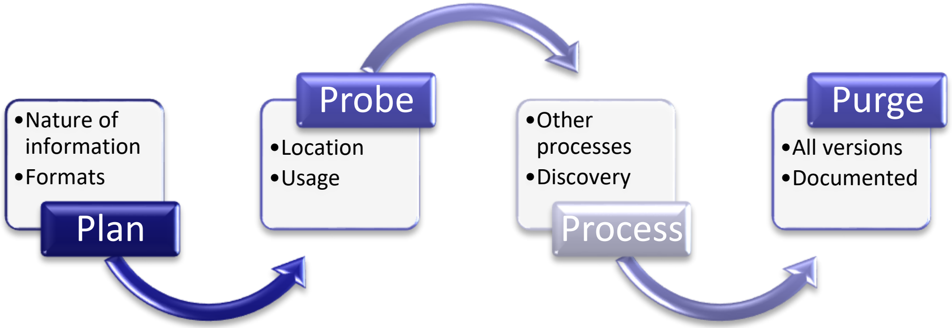
- Implement a change management programme
- Gain input early
- Treat it as a business initiative (Seek benefits)
- Awareness and training are key
  - All people who manage content
  - Administrators
  - Process owners
- Build compliance into KPIs.

People

- Appoint/designate the Information Officer
- Don’t make POPIA compliance an additional/overhead function

Processes

- POPIA 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
- POPIA 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

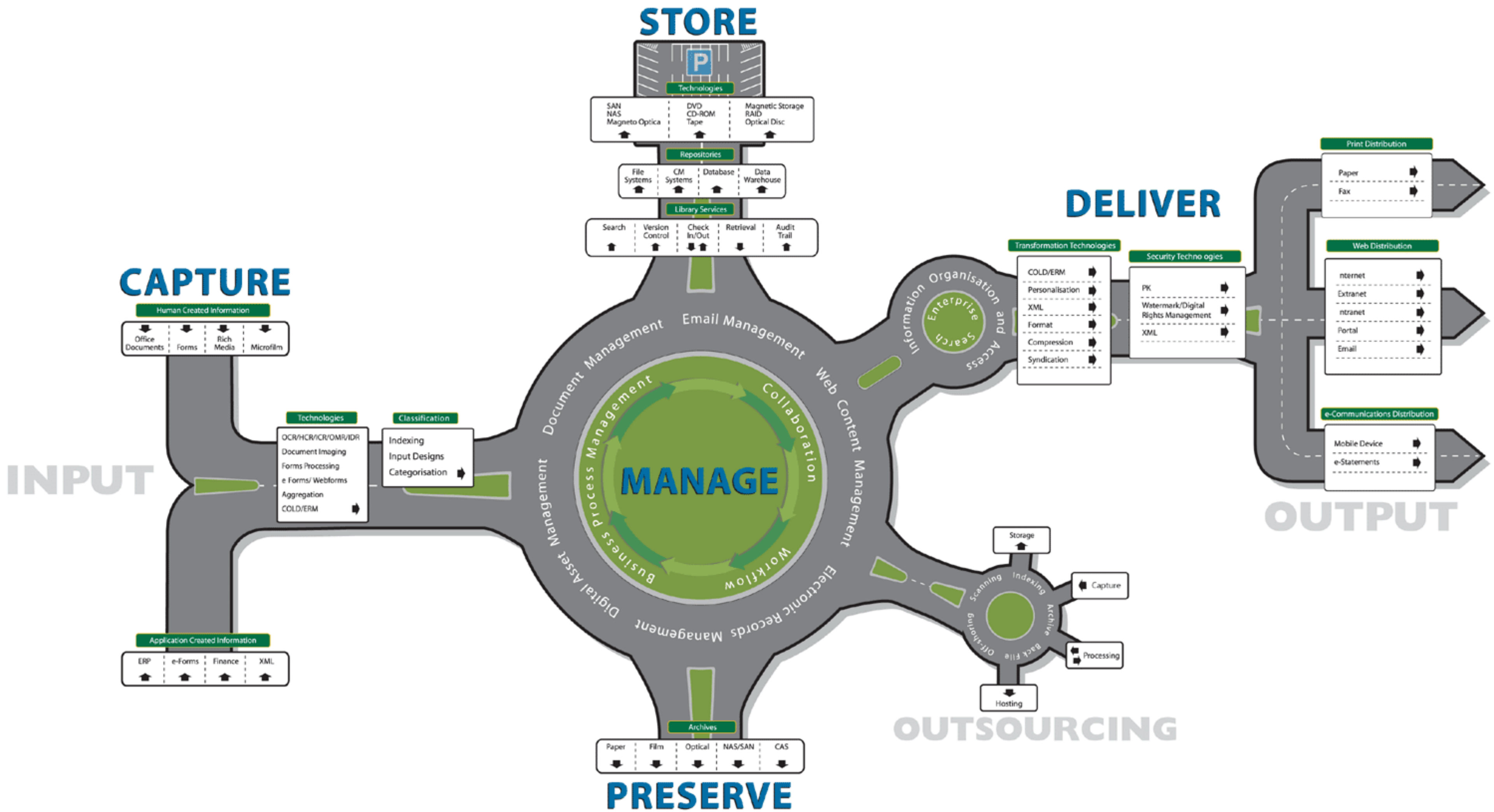
Programme:

Take a Programme Management approach

- POPIA 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.

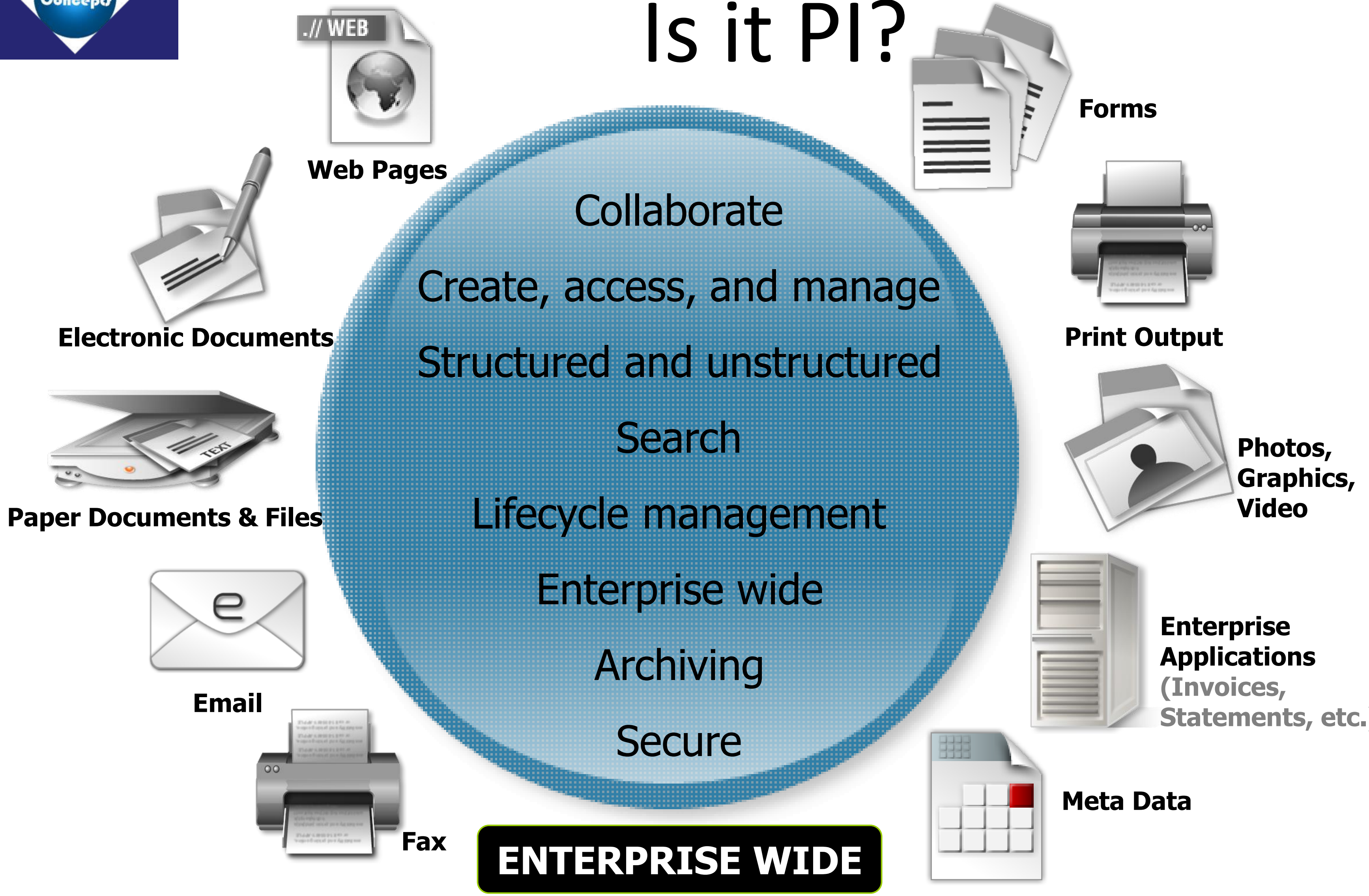
Programmes:

Enterprise Content Management (ECM)

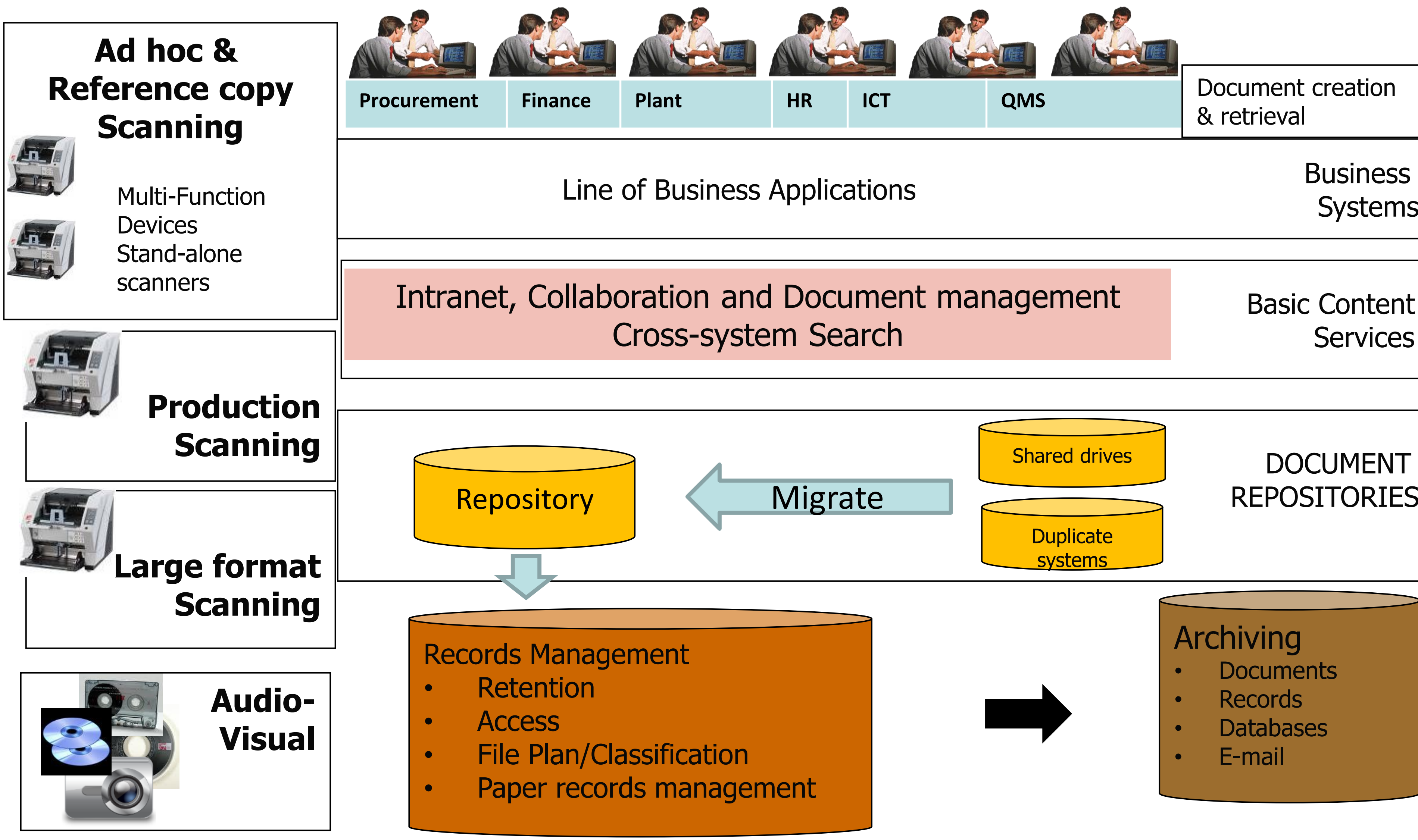


Source: AIIM

What is Content?
Is it PI?



Programmes: Architecture



Limit systems which contain PI

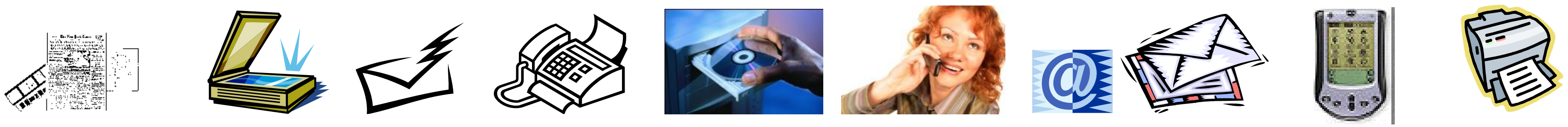
- Keep as few databases as possible
- Automate where possible
  - opt-ins and opt- outs
  - Data checks and validations
  - Disposal processes
  - Cleansing, rationalizing and de-duplicating

Systems should

- Send only to the relevant (opted-in) people
- Cater for disposal
- Meet security obligations
- Keep audit trails of all communication
- Allow for effective reporting

Processes
Flows of information

Internally or externally generated

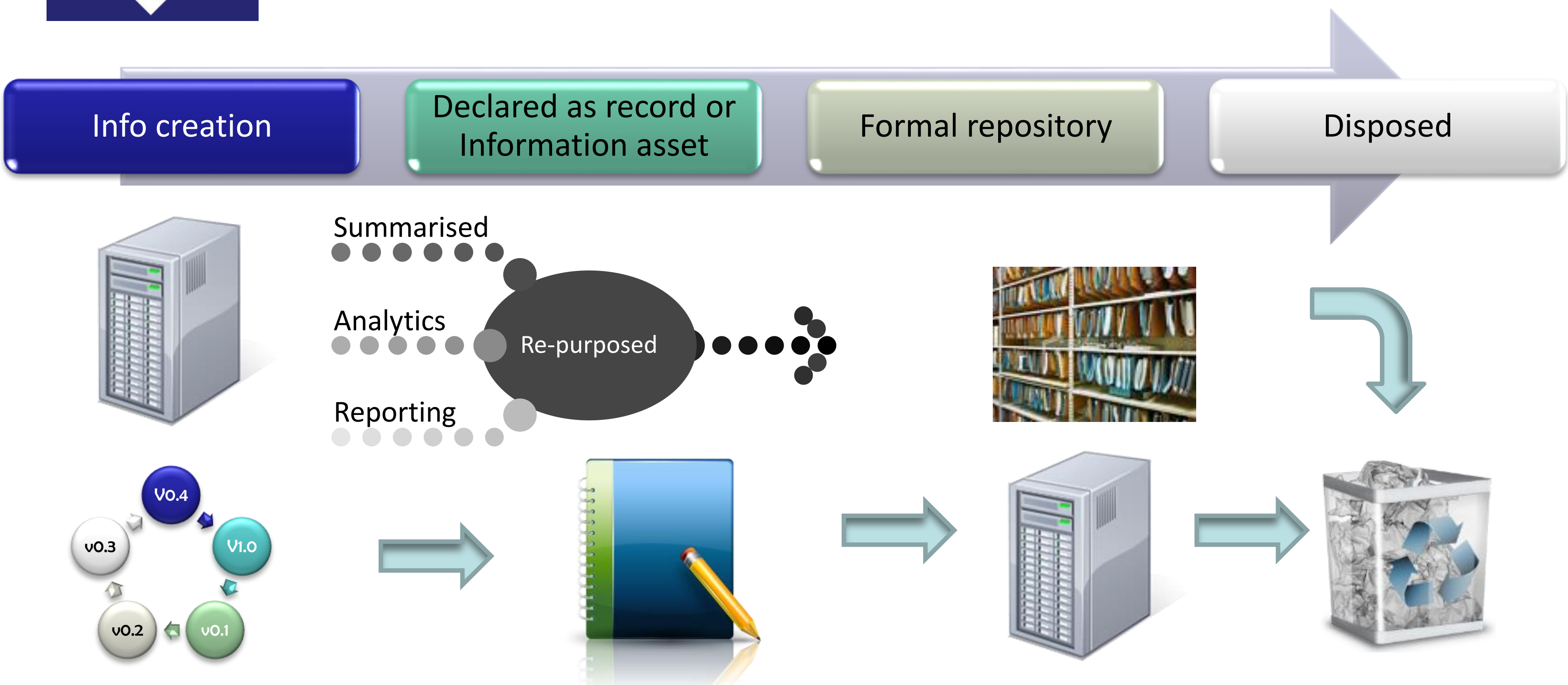


Value determination

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

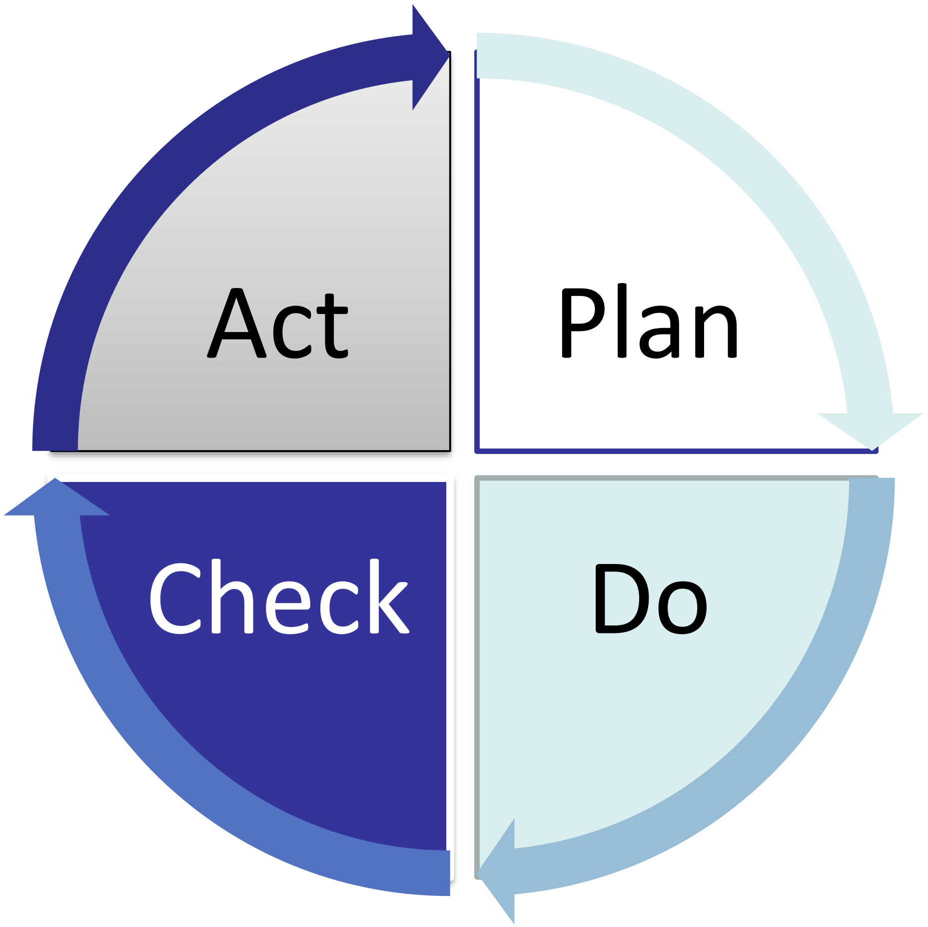


Who creates or receives it
What format is it in?
Should it be converted?
Where is it?
Where can it be stored?
Which processes require it?

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?

Perfect
(Continuous improvement)



Conclusion:
Benefiting from POPIA +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