

# Sustainable information governance

## Responding to the Poynter Report

“Good strategy in this context sets the direction of travel and makes sure that the fundamentals are right...and people, process and technology are the enablers for strategy and need to be changed and shaped over time to deliver it.”

*The Poynter Report – June 2008*



# Agenda

- Why is information governance important?
- Key risk areas
- Data handling procedures
- PwC approach

# Information governance problems affect the entire public sector

37 million items of personal data went missing last year (including the 28 million records lost by HMRC and DVLA):

375 student files

Charity loses 60,000 client records

180 NHS staff payroll details lost

2,800 donors names stolen

6,500 council staff records

# Information governance - why should you be interested?

- Loss of reputation and stakeholder dissatisfaction
- Increasing volumes of sensitive information / data
- Organisations are more frequently transferring and inter-changing data / information
- Regulatory risk
- Organised crime

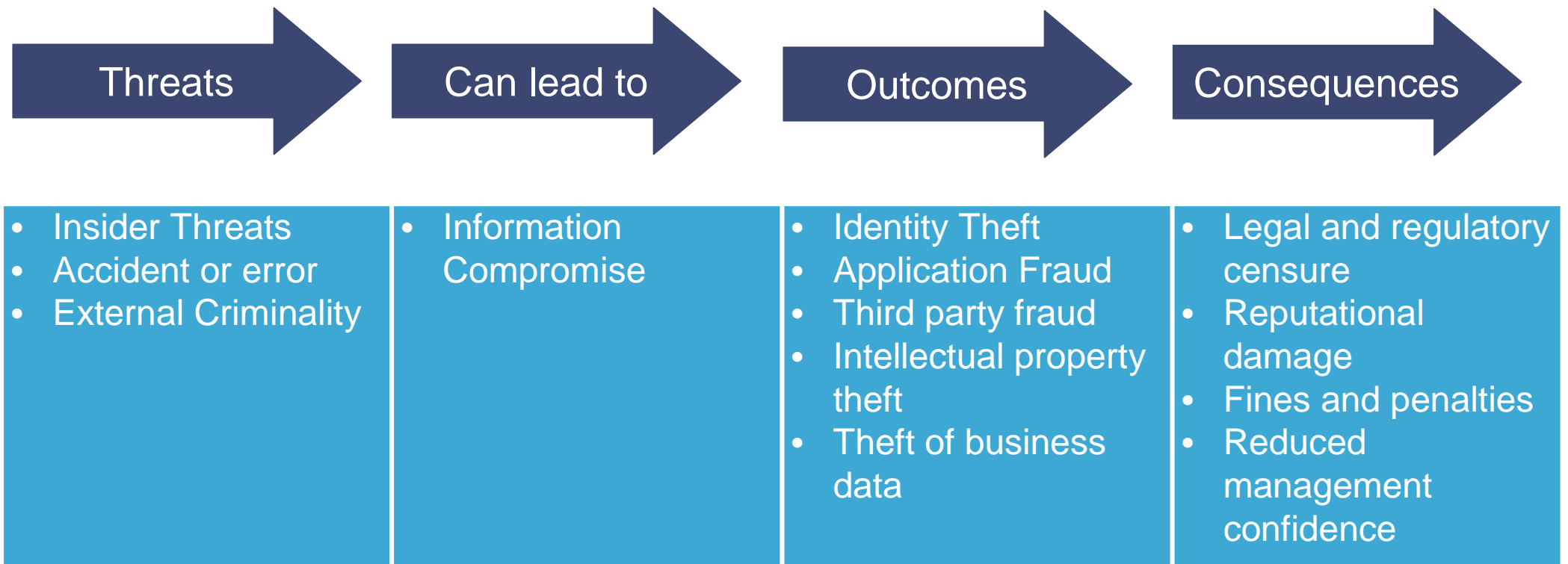
# Information governance - understanding the inherent threat

Get the right balance between **people, process, organisation** and **technology** and understand the risk culture of your organisation

Areas to consider include:

- Laptop and mobile data devices
- Access controls
- Disposal of data
- Call centres

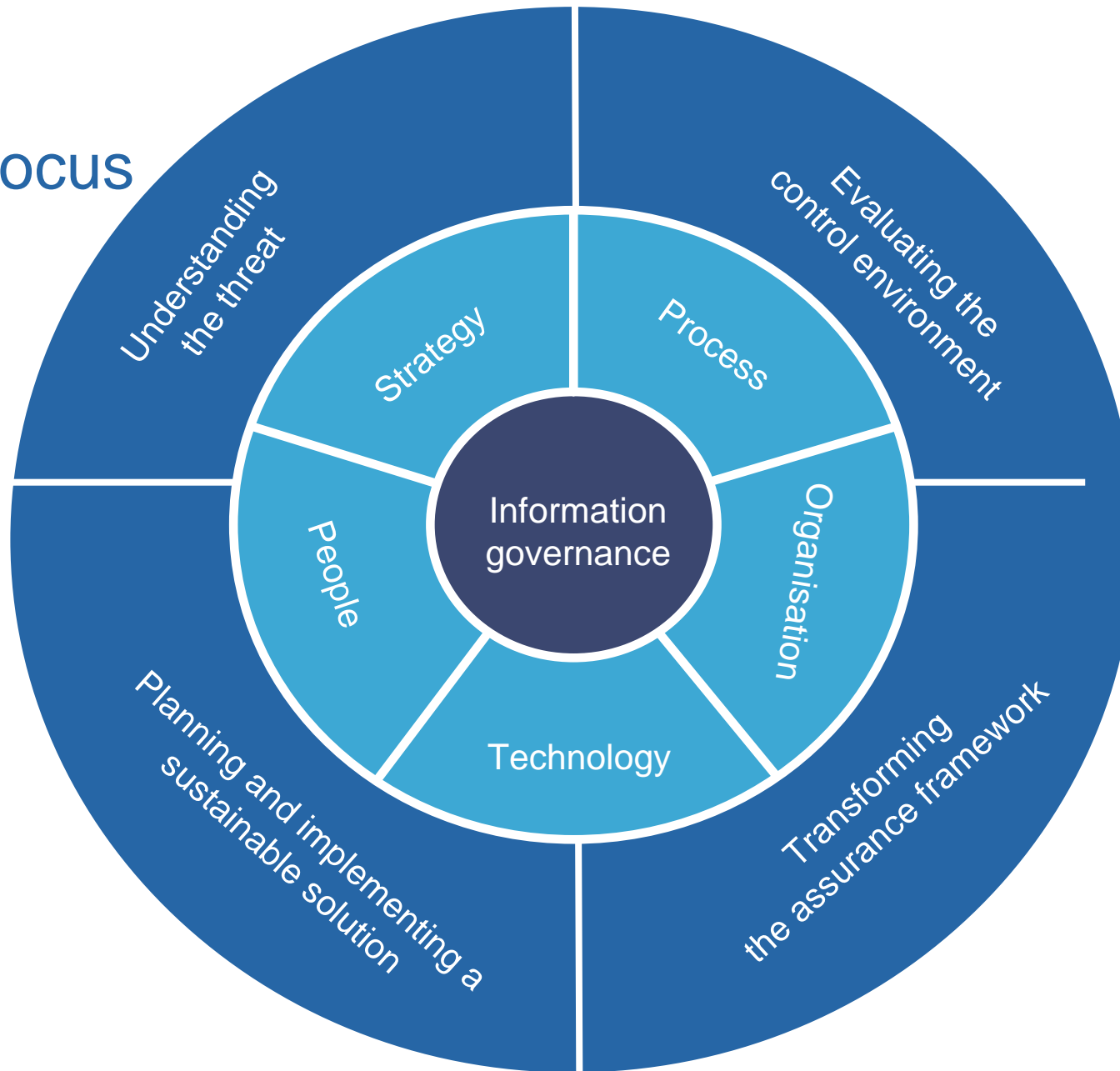
# Information governance - problem on a page



# Information governance

Areas of focus

Key risks



# Information governance - key risk areas

**Strategy** risks to information governance include:

- Tone at the top not set
- Misalignment of business and information security objectives
- Action plans to manage information governance have not been developed
- Budget and resource has not been allocated to support information governance strategies



# Information governance - key risk areas



**Process** risks to information governance include:

- Lack of understanding of end-to-end business process and the risks to information governance
- Lack of process monitoring
- Lack of documented procedures and non-adherence to procedures
- Business processes are not regularly reviewed

# Information governance - key risk areas



**Organisation** risks to information governance include:

- Lack of formal data ownership
- Roles and responsibilities are not defined
- No clear management structure
- Lack of awareness of information governance
- Data sets have not been identified and / or risk-assessed

# Information governance - key risk areas



**Technology** risks to information governance include:

- Technology is not fit for purpose
- Lack of monitoring capability
- Encryption not utilised, or incorrectly utilised
- Inappropriate access controls and password policies

# Information governance - key risk areas

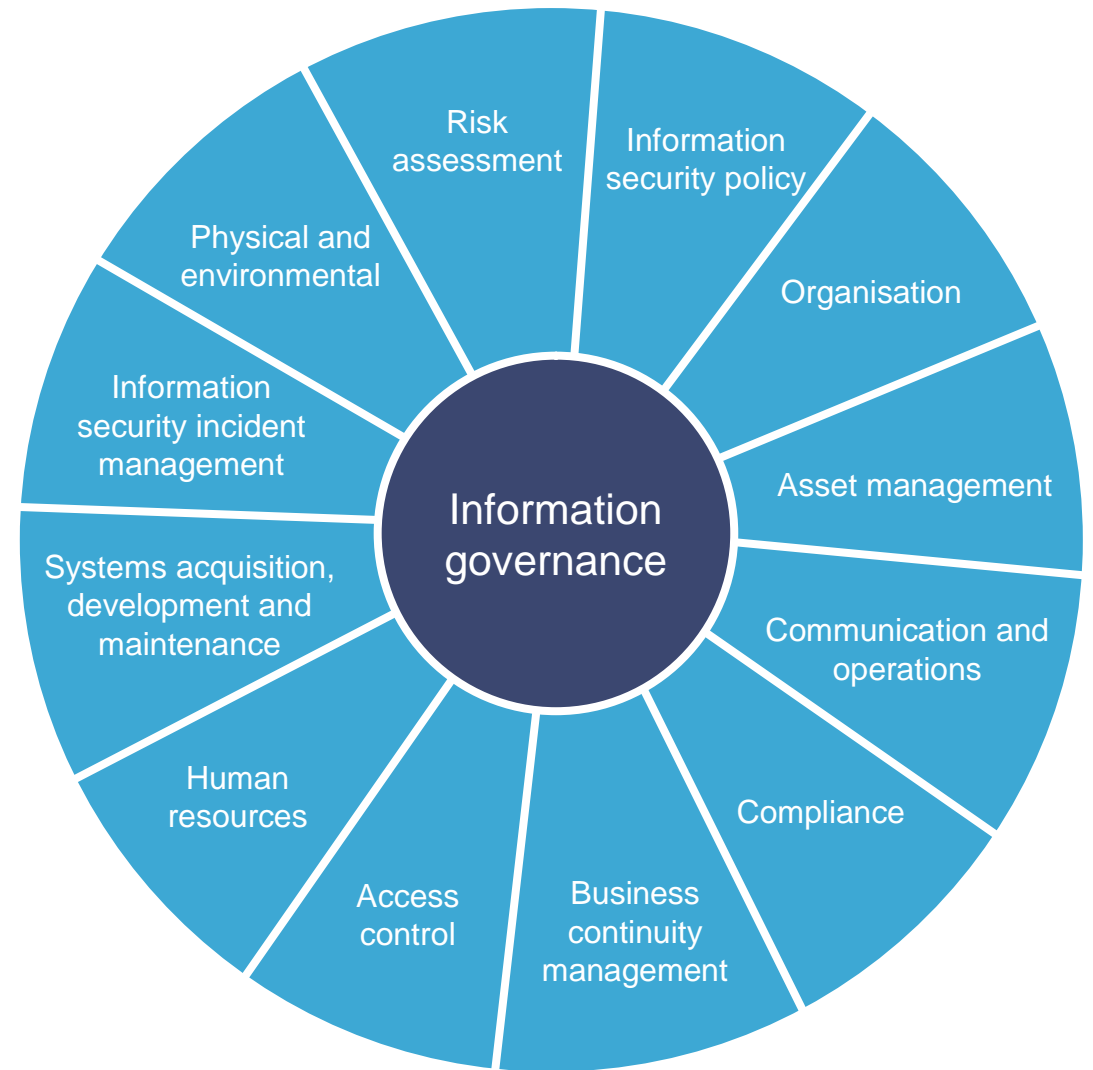
**People** risks to information governance include:

- Information governance training has not been provided
- Job descriptions and procedures do not include information governance requirements
- Roles, accountability and responsibilities are not defined



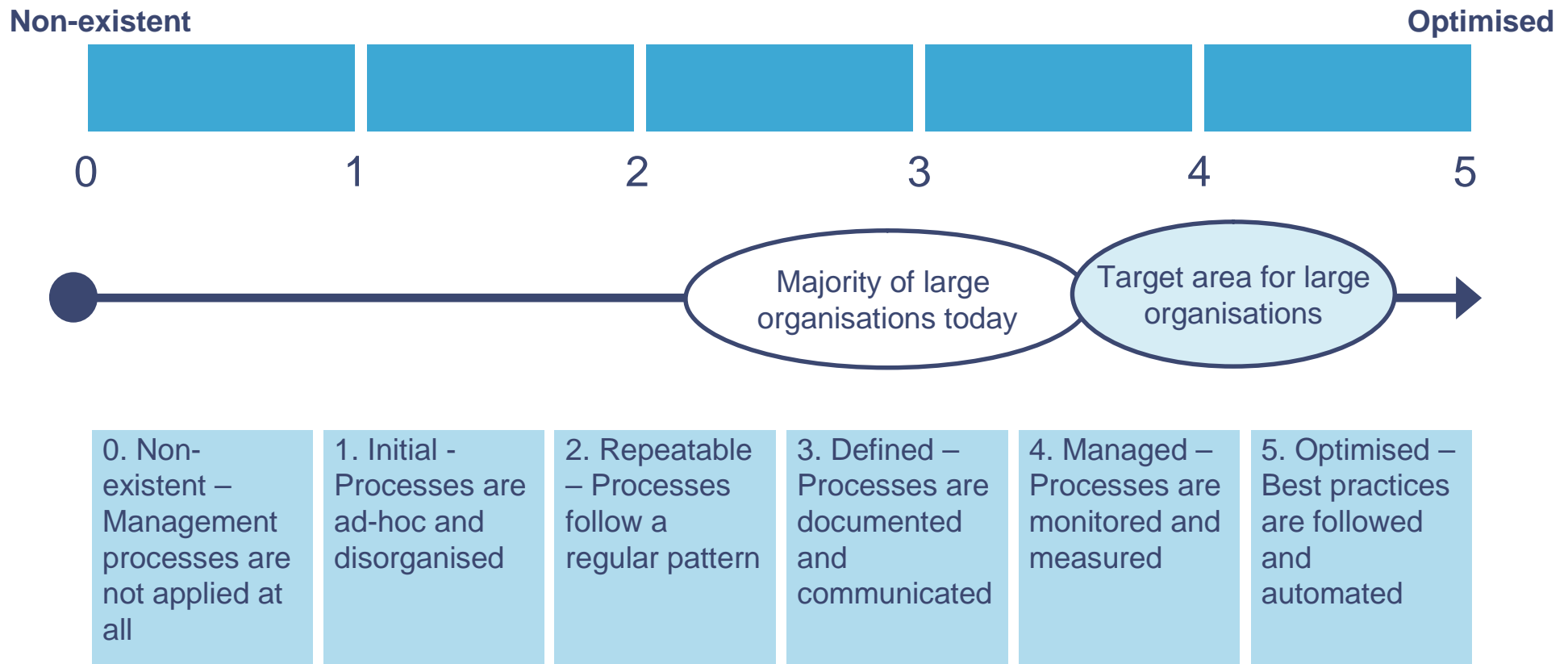
# What does good information governance look like?

Identify weaknesses and target fundamental compliance areas



# Cabinet Office 'Data Handling Procedures in Government'

Measure your maturity



# Cabinet Office 'Data Handling Procedures in Government'

## What does it mean to you?

- Compliance requirement - Cabinet Office guidance will provide the core requirements against which public bodies will be measured;
- Stronger accountability - Ministers have accepted proposals to create criminal penalties to cover the most serious breaches of data protection law after current powers were criticised as being too weak; and
- Four key areas – Core security measures, cultural change, stronger accountability and greater scrutiny.

Central government departments using other public sector bodies and/or third-party providers for delivery must also ensure the requirements are complied with across the entire delivery chain

# Cabinet Office 'Data Handling Procedures in Government'

## Can you answer the following positively?

- Do you have a comprehensive data map?
- Have you risk assessed your datasets to understand the threats that exist?
- Have you assigned responsibility for overall management and security over datasets?
- Have you implemented adequate risk controls and procedures?
- Do controls take into account technology, people and process threats?
- Have you tested security controls and procedures?

If you cannot, there are potentially significant areas of weakness in your management of information governance.

# Cabinet Office 'Data Handling Procedures in Government'

## Timetable for compliance

July 08

Oct 08

- Roll out protective measures through delivery chain
- Change HR policies
- Start cultural change activities
- Formalised information risk policy
- Assigned responsibility

- New systems accredited
- New contracts with providers
- Privacy impact assessments completed
- Greater access controls introduced
- Penetration testing

- Controls in place for information asset owners
- Commenced mandatory training

- During reporting year 08/09, compliance must be assessed annually (SIC)
- There will also be guidance and actions required for local government and other public sector bodies.

# The Poynter review – what did we do?

- Over 5 months, we assessed key parts of the HMRC organisation against information governance industry standards, which had been enhanced by our experience.
- We left the business with detailed controls frameworks that articulated required improvements in organisation, people and culture, process and technology.
- We introduced HMRC to a maturity model based around ISO27002, to guide their future activities in this area.
- We drew on our wealth of knowledge and skills in this area to provide practical support which ‘added-value’ to the organisation.

# The PwC three-stage approach

## Stage 1 - Risk and controls assessment

### **Baseline review**

Series of structured interviews and documentation reviews to baseline the current position. Use PwC's methodology, specifically developed for the HMRC 'Poynter Review' and centred around ISO27002.

### **Gap analysis**

Compare the results of the baseline assessment against the minimum requirements as specified in the 'Data Handling Procedures in Government', ISO27002 and good practice. Assess maturity, develop relevant and practical recommendations to aid compliance.

## Stage 2 – Consolidate plans

### **Plan change**

Develop a prioritised programme of change based on the results of the gap analysis enabling compliance to the 'Procedures' by the deadline.

### **Skills assessment**

Evaluate where the right resources and skills will be deployed to implement the control improvements required.

## Stage 3 – Transformation

### **Implement**

Monitor and track the programme through to completion.

### **Sustain and monitor**

Provide a security and governance framework that will enable ongoing compliance and operation to an acceptable level of risk.

# Next steps – implications and benefits

This is a major process and will involve:

- Cultural change within your organisation
- Defining information governance roles and responsibilities
- Increasing information governance accountability
- Reviewing and potentially changing your business process
- Implementing and embedding new controls

Our approach can assist this process by delivering the following benefits:

- A complete and comprehensive organisation-wide assessment and an enhanced understanding of your current information security environment and risk areas
- Practical and prioritised recommendations to enhance information governance and security
- A sustainable and ongoing programme to provide an organisation-wide approach to information governance

