

Information Governance

Protecting and Sharing Information

25 March 2009



Agenda for today

1. Why is information governance important?
2. The 'Poynter Review' and our approach
3. Are you prepared?
4. Looking forward and setting the direction of travel

“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

Information Governance – Problems affect the public and private sectors

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

45,000 records of personal details lost on route to
Government department

2,800 donors names stolen

6,500 council staff records

Information Governance – Why should you be interested?

Issues	Examples	Consequences
Loss of reputation and stakeholder dissatisfaction	<ul style="list-style-type: none"> • High profile financial sector and UK Government data losses; and • Increasing public concern over security of their bank account and personal data. 	All organisations need to review how information governance is managed
Increasing volumes of sensitive information / data	<ul style="list-style-type: none"> • Student data – personal information; • Employee data – personal data, HR records, pay and bank details; • Financial data – supplier details and bank details; and • Commercially sensitive data – tendering records, supplier pricing schedules and contracts. 	
Organisations are more frequently transferring and inter-changing data / information	<ul style="list-style-type: none"> • Increasing need to share and transfer data with other organisations and third-parties; • Information must be available to support effective operations; and • Organisations need to monitor how third-parties control and process data. 	
Regulatory risk	<ul style="list-style-type: none"> • Payment Card Industry releases Data Security Standard as a compliance requirement; • Regulator fines a financial services organisation £980,000 in high profile notification regarding lost laptop containing customer data; • Developing EU and UK data protection law; and • The Cabinet Office has introduced ‘Data Handling Procedures in Government’. 	
Organised crime and ‘managing in a downturn’	<ul style="list-style-type: none"> • Increased activity by organised criminal gangs targeting customer data; • Price for a single set of identity details – less than £5 on criminal data market; and • Increased fraud risk and a greater need to protect data in a downturn. 	

Information Governance – Understanding the inherent threat

There is a common misconception that information governance breaches occur due to weaknesses in technology or IT security. However, information governance breaches can occur as a result of

- inadequate controls over *technology*;
- weak *processes*; and/or
- inappropriate behaviours adopted by the *people* responsible for handling sensitive data.

We believe it is essential to have an organisation-wide approach to information governance – effective information governance is not just about technology, but requires the right balance between *people, process, organisation* and *technology* and an understanding of the risk culture that underpins the organisation

The Poynter Review

What did we do?

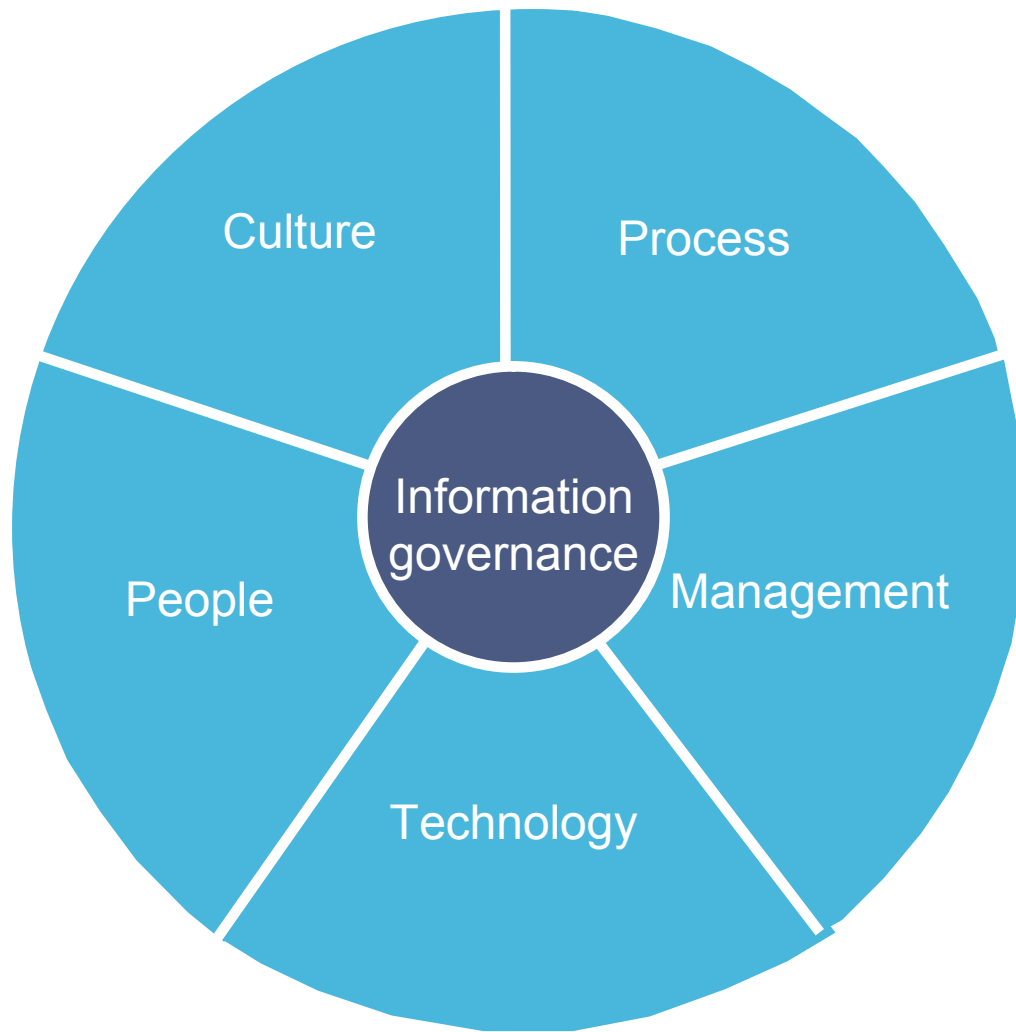
Assessed key parts of the HMRC organisation against information security industry standards.

Provided the business with detailed controls frameworks that articulated required improvements across five dimensions in ***culture, management, people, process*** and ***technology***.

Introduced HMRC to a maturity model based around **ISO27002**, to guide future activities.

Drew on knowledge and skills to provide practical support which 'added-value' to the organisation.

Information Governance – Key risk areas



Key risks to information governance include:

- **Culture** - lack of data ownership, management buy-in or no information governance strategy;
- **Process** - poorly managed operations and business processes;
- **Management** – an organisation-wide approach to information has not been adopted;
- **Technology** - insecure or inappropriately controlled IT environments; and
- **People** - inappropriate behaviours adopted by people.

Information Governance – Being prepared

Can you answer the following positively?

Do you have a comprehensive data map, that outlines:

- What data you hold?
- Where all data is held, and the controls over each data storage location?
- When and how data is transferred between locations?

Have you risk assessed your datasets in order to understand the threats that exist?

Have you identified a senior information risk officer and information asset owners with responsibility for overall management and security over each dataset?

Have you implemented adequate controls and procedures based on the risk to each individual dataset?

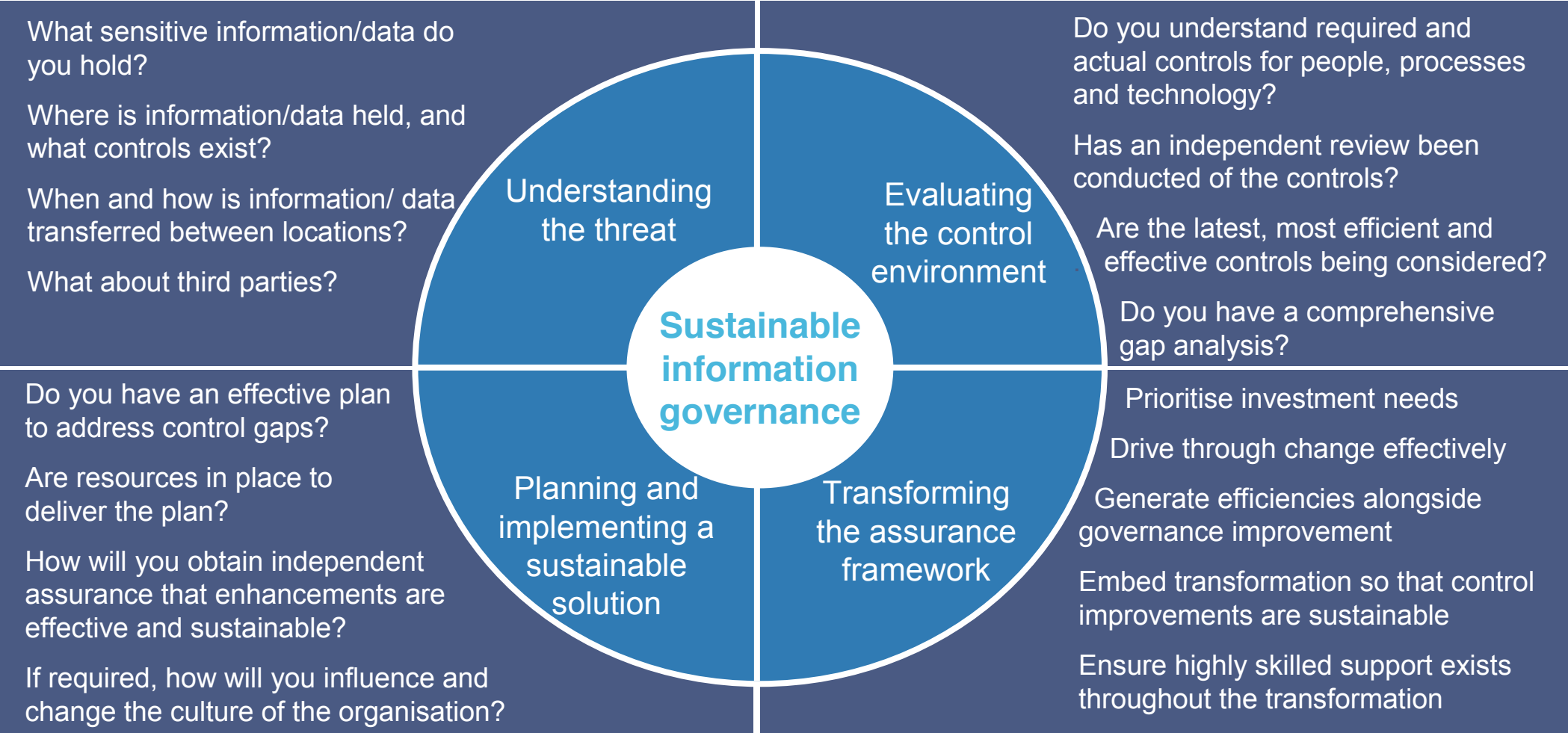
Are the controls adequately focused to the technology, people and process threats?

Have you tested security controls and procedures to ensure that they are effectively mitigating the key risk exposures?

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

Information Governance – Areas of focus

Information governance should be at the heart of the organisation’s strategy and effectively underpinned by the culture, technology, people and processes in place



Information Governance - Project risks

Information governance is not just a risk for 'business as usual':

- Projects which involve changing the way data is processed and managed should be risk-assessed;
- Information governance should be built into project plans; and
- Privacy impact assessments (PIAs) are mandatory for central government and are good practice for the private sector and wider public sector.

*The PIA process will identify **privacy issues** early and enable organisations to address issues effectively, quickly and inexpensively, rather than becoming major problems later on in development.*

Information Governance – Setting the direction of travel

Information governance – next steps?

- Risk-based approach;
- Multi-dimensional view of controls – not just IT;
- Not just a point in time exercise;
- Project risks;
- Provide challenge to your organisations; and
- Compliance and assurance programme.

Questions?

Contact details

Jen Duck

jennifer.duck@uk.pwc.com

0191 269 4258

