

The value of an information governance strategy

April 2014



Organisations know they need to act on information risk but do not know where to turn or what to do next

In June 2013, PwC and Iron Mountain published the second Information Risk Maturity Index. The key finding of our report was the need for a strategic focus for improving information management.

Our survey found that almost half of organisations still need to significantly improve their information management practices. Even organisations that lead the way in addressing information security are struggling with information retention and are just as likely to keep everything ‘just in case’.

Issues of compliance affect every organisation. The scale of an organisation, the nature of its business, its technology adoption and its global reach increase its likely compliance vulnerability.

Effective governance balanced against risk forms the bedrock of efficiently dealing with these challenges. Positioning information governance as a solution in the compliance armoury of a business is essential. Conversely, treating it as a plug and play technology solution to a perceived technology problem will increase the chances of failure.

36%

***keep all
information just
in case***

Good information governance is far more than an information technology problem

Technology programmes addressing information management issues often fail because of poorly defined strategy, lack of adequate governance or support, missing or ineffective policy and procedure and poorly or inadequately executed change management.

They rarely fail because of technology inadequacies, rather the inadequate definition of requirements, due to lack of strategy, which leads to poor purchasing decisions.

Exposure to information risk needs to be reduced which needs action from the top

Taking a holistic approach

Gains in awareness should be transformed into a strategy and set of actions to reduce exposure to information risk. Putting strategic value to your information assets allows you take greater control and invest in protection of what has the greatest worth. The drivers for improved information management equate to the impact that a failing may have.

This is supported in the study which highlights that the biggest concern from a data breach is reduced customer loyalty and the impact on brand reputation. This far outstripped the concern over any legal consequences.

Understanding your organisation’s objectives for the management of information in the context of overall business goals is fundamental to producing a strategy that will achieve its long term aims. This requires buy-in and involvement from the very top of the organisation.

By engaging key stakeholders across your senior executive teams, it is possible to gain an understanding of, and form a view to, the context and drivers affecting information management within your organisation.

Where to start?

An effective strategy should provide flexibility for your organisation to adapt to new demands for information management. This comes down to:

- Making a set of choices about how you want to operate and what priorities you should address taking into account business, competitive, regulatory and compliance drivers.
- Understanding how you currently tackle information management and what gaps exist to meet a desired end state will provide a focused plan for improvement.
- Prioritising the plan according to risk will help define the ‘must have’ objectives.

Periodic reviews, controls, checks and measures. This measures ensure that the strategy remains aligned with your corporate objectives providing defined requirements for new policies, assessing existing systems or implementing new ones.

Making strategic choices early, proactively and in a transparent way reduces uncertainty that can often paralyse an organisation during later implementation phases

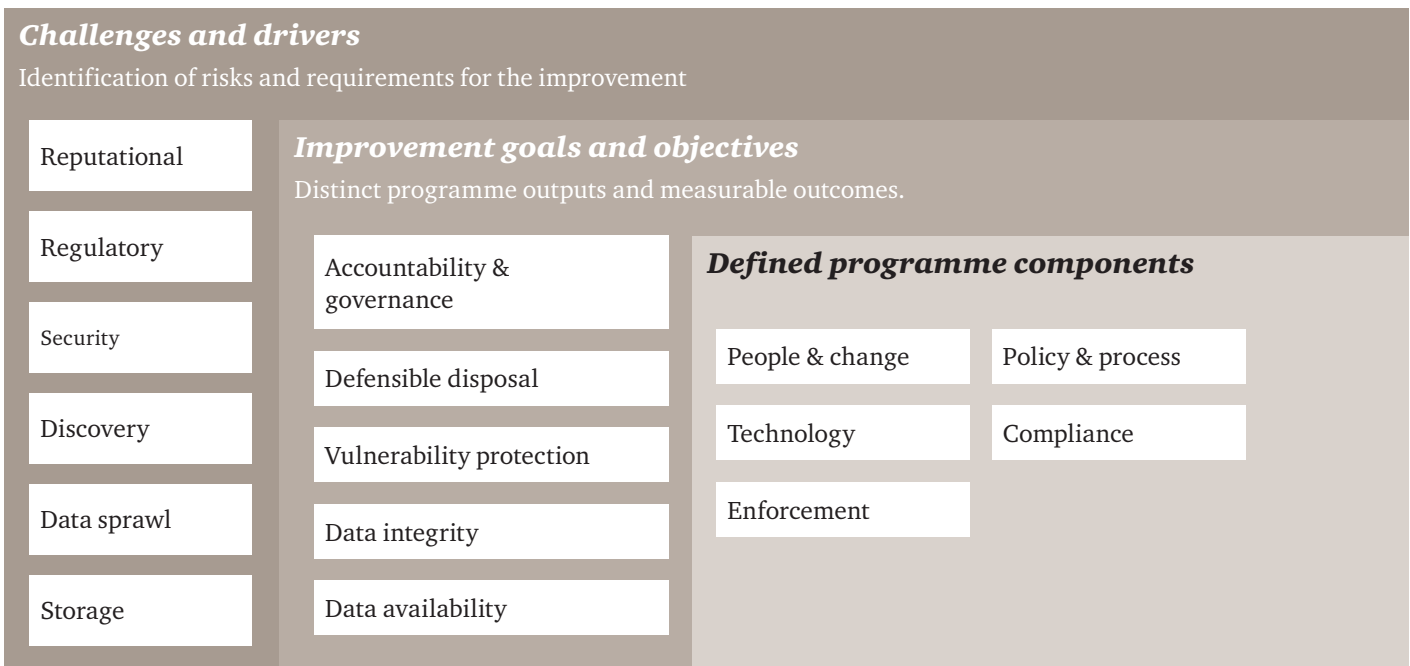
Putting the strategy into action

An information governance strategy pieces together initiatives in the areas of:

- Legal and compliance
- Information architecture
- Data privacy
- Data retention
- Information security

- Knowledge management
- Information sharing
- Information quality and assurance
- e-Discovery

A roadmap provides important direction for your stakeholders. Showing how you plan to implement the strategy and the key elements of your programme.



Greater control of information through a governance strategy helps mitigate risk by directing investment in the protection of information that matters to you most.

“Information governance brings together key stakeholders from your senior executive teams to form a holistic view to the context and drivers affecting how information is used and managed within your organisation.”

When you come to writing policies, changing the way people work or implementing systems, having a strategy in place provides the reference point for what you are doing and why

Achieving success

Your information governance strategy and its supporting programme become effective if leadership embeds improvement within the culture of the organisation through support and enforcement.

The value of the strategy depends on being able to sell it back to the business. Priorities and objectives should be put into context against business drivers, cost, risk and time.

Success is achieved as much by senior stakeholder support through sound governance, as by adequate policy and procedure and auditability of the implementation.

Contacts

Tom Lewis

Partner

+44 (0)20 7213 5911
tom.e.lewis@uk.pwc.com

Umang Paw

Partner

+44 (0)20 7804 4347
umang.paw@uk.pwc.com

Gavin Siggers

Senior Manager

+44 (0)20 7804 4026
gavin.d.siggers@uk.pwc.com

Nicholas Conway

Director

+44 (0)20 7213 3556
nicholas.p.conway@uk.pwc.com

“Poor information practices expose the enterprise to a variety of risks potentially leading to significant financial penalties and reputational loss.

Understanding what information you need to keep and how you can improve the way it is managed reduces these risks and prepares you for scrutiny. ”

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PricewaterhouseCoopers LLP. All rights reserved. In this document, “PwC” refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

140411-163936-KV-OS