

Information Risk Management: Valuing, Protecting and Leveraging Business Information

ROBIN SMITH



Information Risk Management: Valuing, Protecting and Leveraging Business Information

is published by Ark Group



UK/EUROPE OFFICE

Ark Group Ltd
Paulton House
8 Shepherdess Walk
London N1 7LB
United Kingdom
Tel +44 (0)20 7490 0049
Fax +44 (0)20 7324 2373
publishing@ark-group.com

NORTH AMERICA OFFICE

Ark Group USA
4408 N. Rockwood Drive
Suite 150
Peoria IL 61614
Tel +1 309 495 2853
Fax +1 309 495 2858
publishingna@ark-group.com

ASIA/PACIFIC OFFICE

Ark Group Australia Pty Ltd
Main Level
83 Walker Street
North Sydney NSW
Australia 2060
Tel +61 1300 550 662
Fax +61 1300 550 663
aga@arkgroupasia.com

Commissioning editor

Anna Shaw
ashaw@ark-group.com

Design and layout manager

Danielle Filardi
dfilardi@ark-group.com

Managing director

Jennifer Guy
jguy@ark-group.com

UK/Europe marketing enquiries

Robyn Macé
rmace@ark-group.com

US marketing enquiries

Daniel Smallwood
dsmallwood@ark-group.com

Asia/Pacific marketing enquiries

Steve Oesterreich
aga@arkgroupasia.com

ISBN: 978-1-906355-85-2

Copyright

The copyright of all material appearing within this publication is reserved by the author and Ark Conferences 2010. It may not be reproduced, duplicated or copied by any means without the prior written consent of the publisher.

Chapter 1: Information risk management – Key concepts and issues

Why information matters

Information is the currency of the modern organisation. It should be valued and managed as carefully as all corporate resources. But what happens if the value of information is not recognised by organisations? What if the risks and threats arising from the poor management of information are dismissed as unimportant? What risk does this present to the successful delivery of services by any organisation?

The response to these questions defines how an organisation equips itself to deal with information risk. Information risk management (IRM) is an approach to organisational development that values information and the threats to, and vulnerabilities of, this most valuable asset.

Information risk management is a vital part of any organisation's business development and improvement strategy. Information risk management protects business-critical capabilities from risks, threats and issues. Initiating regular scanning, assessment and development of all information risks facing an organisation achieves this result. For example a specific information security risk relates to the prevalence of malware on the World Wide Web. Good information risk management identifies this as a threat and demands an ongoing response from information security professionals to protect the organisation from this threat.

Information risk can be identified as part of every organisational activity and

can never be eliminated, nor can all the information risks ever be known. Information risk in itself is not bad; it is often essential to progress. But information professionals must learn to balance the possible negative consequences of risk against the potential benefits of its associated opportunity. IRM not only enables an organisation to scan and manage risks but good information risk management can turn negative risks and threats into valuable business intelligence to drive improvement.

Information risk management is ultimately an approach to managing and valuing business information across an array of instances, from new information systems to external legislative demands. Key outcomes from improved IRM include higher-quality knowledge assets, reduced costs and higher productivity from better-informed staff.

In an uncertain time for the global economy, how an organisation establishes its information risk management strategy and capability could be the difference between prospering and going under.

Defining information risk management

Information risk has been on the rise over the last few years as technology, economics and customer expectations change. Information risks are defined as those items that have a net negative impact on an organisation, based on reviews of probability and impact of the occurrence. Information

risks include security threats from malware, data breaches or failure to implement standards or best practices.

Previous conceptions of IRM related purely to security risks from malware and other technology related threats. However this misses a critical point that establishes IRM as a key part of any organisational development and improvement project. IRM is the organisational approach that critically values business information assets in the same fashion as physical assets. This allows an organisation to understand all the dimensions arising from managing business information.

IRM is recognised as the discipline that identifies, classifies, values and controls organisational information to manage risk and opportunity, thereby enhancing its value to the organisation.¹ One example of information risk and its management to enhance its value relates to monitoring for legal changes impacting a business. A change in law or regulatory requirements will demand a response to integrate these changes into company services. A failure to identify and respond to this key form of information risk could result in a company being fined or having its corporate reputation damaged. One example of organisations failing to respond to information risk is in response to disability discrimination legislation in the UK where new regulations required all public authorities to promote equality of opportunity for disabled people via improved access to services.²

There are a number of key terms relating to IRM:

- **Information** refers to all types and forms of business information obtained, recorded or processed by the organisation, including

personally identifiable data and corporate intelligence;

- **Information risk** is the form of risk which impacts the management and valuation of business data, information and knowledge assets;
- **Intelligence** is defined as information that has been subject to a defined evaluation and risk assessment process in order to assist with organisational decision making; and
- **Information risk assessment** relates to the overall process of information risk identification, analysis and evaluation.

IRM is essentially a structured approach to the management of threats and opportunities facing an organisation. It uses a range of improvement techniques including information policy, procedures and practices in order to support the completion of the tasks of identifying, analysing, evaluating, controlling and responding to information risks.

Trends in information risk

A recent survey of corporate risk professionals revealed the growing concern regarding the continued neglect of the value of business information.³ From financial markets to public services, a range of opinion was sought on the impact of the global recession and what this would mean for risk management, particularly positive risk-taking within sectors. A sample of risk professionals highlighted that the decline in positive risk-taking had been evident since 2008. Fewer than 25 per cent of risk officers sampled stated that individual organisations were prepared to consider risk-taking in a tough economic environment.

These findings contrast with research into success psychology that states that organisations should be willing to innovate just as much during a recession as during

prosperous times. Information professionals who are seeking to introduce improvement techniques should consider corporate attitudes to innovation in order to harmonise new initiatives with strategic plans. This will avoid clashing with corporate planners who are seeking to avoid and reduce risk-taking at certain times.

The range and costs of information risk

In this era of exploding volumes of digital content, it is vital that an organisation learns how to raise the value of all its information assets through IRM. So far there have been few answers to the problems presented by information risk, which is ultimately about sustaining the intellectual capital available in a range of documents and files that might not be captured in an information management system, to the benefit of the organisation and its customers and stakeholders.

Information risk can be classified in accordance with a simple taxonomy, allowing information professionals to tag different types of risks for ease of reference. The proposed taxonomy for information risks is:

- **Strategic** – This type of information risk relates to risks and threats to the strategic position of an organisation, including economic and legal threats and risks. For example, updates to legal compliance required by the introduction of new laws in relation to flexible working for staff present a strategic planning risk for an organisation that is not able to adapt to new statutory requirements.
- **Operational** – These relate to risks and threats impacting the operation of an organisation including staff skills shortages which might demand

significant investment at a time when finances are limited.

- **Financial** – Economic and capital threats are of primary concern and will include loss of earnings, limited finances, fines or other related financial issues. A specific financial risk is the level of capital available for investment. If there is no capital available then there is a limit to the research and development possible to develop new product to secure an organisation's commercial position.

As is evident, risks can be characterised in a number of different ways. The aim is not to prescribe how information risks should be characterised but rather to capture and assess the diversity of threats and opportunities facing an organisation.

For more information on the taxonomy of information risk, see Chapter 2.

The management of information risk is an essential activity, illustrated by some highlights from recent Dynamic Markets research:⁴

- Fifty-five per cent of staff store work-related files such as e-mails and files in locations other than a shared drive;
- One in six employees lies to cover up mistakes caused by using the wrong version of a document; and
- Sixty-three per cent of employees say incorrect information has resulted in negative consequences.

The value of all types of information and associated risks can fluctuate and if day-to-day business across an organisation is interrupted, the loss of value can be excessive.

Avoiding unnecessary costs is just the starting point for IRM. Information penetrates every service and activity within an organisation and must be managed

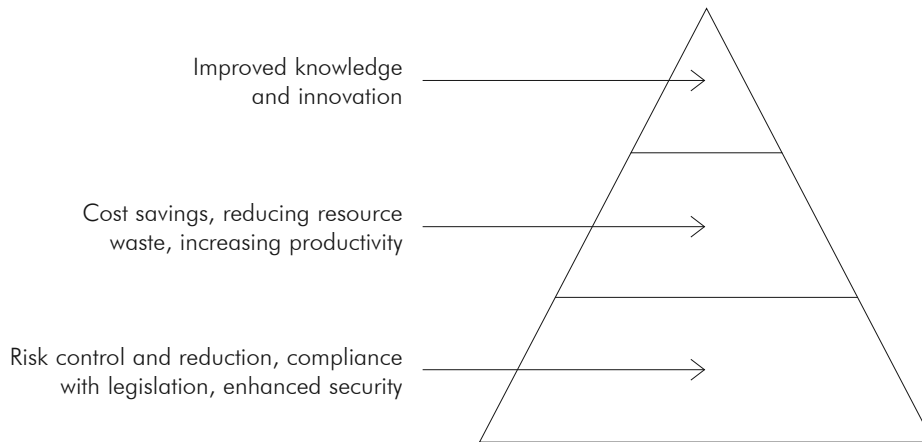


Figure 1: The hierarchy of benefits from improved IRM

to enable better communication and collaboration. Figure 1 presents the array of benefits from improved IRM.

Better IRM also allows an organisation to deliver myriad benefits including:

- **Integration with corporate strategy development** – Scanning for external information risks can help corporate strategists to develop agile and responsive programmes that are future-proofed.
- **Enhanced performance management** – Better information products are essential to information risk reporting and quality auditing to raise standards.
- **Reduced operating costs** – By reducing duplication and the ongoing retention of orphan records through improved information risk scanning, an organisation can make substantial savings to its digital storage costs.
- **Improved communication and collaboration** – Better quality information can be shared and re-used by staff with confidence to improve networking and collaboration.
- **Proactive planning** – Responding to information risk is reactive. Better planning can place information

professionals in a position to have full view of upcoming risks and threats.

The ultimate objective for IRM is to deliver high quality information products. This can help build improved business intelligence. Creating quality business intelligence can drive improvement and deliver organisational development. IRM provides both the necessary tools and supporting techniques to manage the value of business information and in turn create business intelligence.

Principles of information risk management

Information must possess authenticity, reliability, integrity and usability in order to be considered of high quality. Good quality information is essential for sound decision-making at every level of an organisation and is a core element of performance management. It is vital that the performance information used to inform, manage and plan activities is accurate, reliable and comparable.

Recent analysis of a range of organisations suggests that the quality of information underlying corporate information is variable across the information sector. This needs to be improved.

A number of principles underpin the approach proposed using the integrated IRM framework. These establish quality and reliability of outcome from using the techniques outlined. The principles are that the approach is:

- **Evidence-based** – It is vital to base information risk analysis and planning on clear research evidence;
- **Consistency** – Accuracy and integrity are prerequisites for information risk products to deliver a consistent service;
- **Skills focused** – Only via competency and experience will staff involved in planning be able to spot and handle information risks expertly; and
- **High quality** – The characteristics of information assets required to reduce risk will raise quality to the highest standards.

By adopting these unifying principles, information professionals can establish the requirements for all business information. The principles also provide a rationale for talking about IRM as a key organisational development activity.

IRM integrated framework

Scanning, assessment and development are the critical steps within IRM, forming a cycle of activity for information professionals. By linking these steps, an integrated IRM framework can be developed which can provide a number of products for an organisation, from a corporate risk and threat assessment to policies and action plans for improvement. Current practice often leads to intelligence gathered from scanning not being integrated into policies and action plans at the development stage. The integrated IRM framework resolves this problem by allowing a series of five

techniques to be considered as part of a total approach to information risk.

Using this approach to integration IRM can be positioned as a strategic process that governs the management of information risk from initial identification to final resolution and performance reporting. Positioning IRM strategies within an organisation can determine the success or failure of a risk initiative.

Strategic control of information risk is a crucial dimension of an information risk strategy. IRM provides a critical controlling strategy for the key information assets within an organisation. By exerting control over information risks where possible, the organisation can begin to be proactive in dealing with threats and issues likely to have a positive or negative impact on services.

Control is one dimension of IRM. Creating quality information and business intelligence is another. Business intelligence can drive improvement and deliver organisational development. IRM provides both the necessary tools and supporting techniques to manage the value of business information and in turn create business intelligence.⁵

Information risk management can become a key tenet of all organisational risk and assurance activities, integrating easily with performance and organisational development strategies. It is a continuous cycle designed not only to identify, assess, manage and review risks, but also to support the strategic planning process. A number of leading organisations across the UK and Europe have begun to recognise the impact of failing to manage information risk. From industries as diverse as policing and the pharmaceutical industry, a new approach to information risk management has emerged, focusing on valuing and developing business intelligence.

Integrated IRM provides the techniques and tools for significant improvement

in an economic climate that demands improvement and innovation without incurring costs and resources.

Information, innovation and risk-taking

Finally a word or two on the conceptions relating to risk. Too often when risk is discussed it is in purely negative terms. Risk is only mentioned as a threat, a problem or a negative concept. Organisations therefore often think of risk as something to avoid. This is a mistaken approach to information risk management. Information professionals need to adopt a new mindset and approach to the idea of information risk. This new approach needs to cast risk in much more illuminating and accurate terms. Information risk must be seen as having several dimensions. A common philosophy amongst risk professionals states that ‘without risk there is no reward’. Tony Giddens, sociologist and author of *The Third Way*, has written some illuminating work on the conception of risk and the tendency to miss the positive aspects relating to opportunity and innovation.⁶ Giddens states that “opportunity and innovation are the positive side of risk”. This is undoubtedly correct. IRM within leading organisations places a premium on understanding that there are two aspects to risk – both positive and negative, as outlined in Figure 2.

So IRM is not just about dealing with threats and disruptions; it might be possible to take positive risks such as introducing social media technologies to help staff share knowledge and make connections across departments. Organisations will concern themselves with the management of threats but information professionals must begin to seek opportunities to innovate and improve. For more insights into information risk and innovation see Case study 2.

Information professionals must be risk-takers. Opportunities to innovate are

Opportunity	Innovation
Security	Responsibility

Figure 2: The risk matrix

rare for organisations that are stating that the recession is limiting research and development budgets. Information risk presents itself in a variety of forms, from security threats to new government funding for social media pathfinder projects. Active scanning and assessment can provide the platform for new ways of thinking, working and delivering services. Information professionals must seek to control threats whilst considering where an organisation can capitalise on new opportunities or ideas.

References

1. Forrester, ‘Information workplace trends 2007’, February 2007. Available at http://www.forrester.com/rb/Research/information_workplace_trends_2007/q/id/42796/t/2.
2. Mitchell, E., ‘Legal Update 4 March 2010 on challenges to cuts’, communitycare.co.uk, 4 March 2010. Available at <http://www.communitycare.co.uk/Articles/2010/02/25/113898/legal-challenges-to-council-cuts-in-services.htm>
3. Smith, R., ‘A Model for Information Risk’, Northumbria University, 2010 (unpublished).
4. Dynamic Markets for Tower Software, ‘Document Mayhem in the UK and Republic of Ireland’, 2007.
5. Chaffey, D. & Wood, S., *Business Information Management; Improving Performance using Information Systems*, FT Press, 2004.
6. Giddens, A., *The Third Way: The Renewal of Social Democracy*, Polity Press, 1998.