

Information Risk Management: Valuing, Protecting and Leveraging Business Information

BY ROBIN SMITH



Contents

Executive summary.....	VII
About the author.....	IX
Acknowledgements	XI
Part One: Understanding and implementing information risk management	
Chapter 1: Information risk management – Key concepts and issues	3
Why information matters.....	3
Defining information risk management	3
Trends in information risk.....	4
The range and costs of information risk.....	5
Principles of information risk management	6
IRM integrated framework.....	7
Information, innovation and risk-taking.....	8
Chapter 2: An introduction to the IRM improvement techniques	9
Getting started.....	9
Information risk strategy	9
Key linkages	10
Introducing improvement techniques	11
The benefits of integration	12
Impact and results.....	13
Chapter 3: Technique one – Information risk scanning.....	15
Overview	15
Quality information.....	15
Information, intelligence and corporate memory.....	16
Getting started.....	16
Scanning criteria.....	17
Taxonomy of information risks.....	18
Scanning key elements	19

Chapter 4: Technique two – Information risk management assessment	25
Introduction	25
Information risk control and assessment tool	26
Step one – Ratify information risk priorities.....	27
Step two – Assess individual information risks.....	28
Step three – Controlling information risk.....	28
Step four – Monitoring information risk.....	29
Step five – Reviewing and reporting.....	30
Step six – Communication and learning.....	30
Chapter 5: Technique three – Information and intelligence development	33
Overview	33
Evidence based policy-making	33
Current policy guidance	34
Information policy definitions	35
The policy cycle	35
Policy assessment questions	36
Supporting methods	39
Chapter 6: Technique four – Defining the value of information	41
Overview	41
Information capitalisation	41
Principles of capitalisation.....	42
Valuation method.....	43
Communicating information value	45
Chapter 7: Technique five – Improving information risk governance and assurance	47
Overview	47
Corporate governance and assurance.....	47
Delivering improvements	48
Governance structure, roles and responsibilities	48
Information assurance auditing	51
Building competency	52
Chapter 8: Information risk management – The integrated framework	55
Overview	55
Benefits of integration.....	55
Linking techniques.....	56
Governance and assurance	57
Proactive or reactive control strategy	57
A learning organisation?	58
The future of information risk	58

Part Two: Case studies

Case study 1: Global pharmaceutical company – Adopting innovative digitisation strategies to deliver cost savings	63
Overview	63
Revising information strategy.....	63
Merging services and skills	64
Information risk assessment processes	64
Defining digitisation approaches	65
Confronting problems	66
Communication and collaboration.....	67
Lessons learned	68
Conclusion.....	68
Case study 2: Eight lessons in information risk, innovation and learning from technology strategists	69
Overview	69
Innovation and information risk.....	69
Eight lessons to learn	69
Summary.....	72
Case study 3: UK local government – Improving information risk governance and performance	73
Overview	73
Demands for improvement	73
The problem of governance.....	74
Implementing IRM.....	74
Appointing information risk officers	74
Issues and risk reporting	75
Security, governance and culture.....	75
Lessons learned	76
Case study 4: UK police force – Information risk and intelligence scanning	77
Overview	77
A new approach to criminal and business intelligence	78
Benefits of NIM.....	78
The force’s NIM strategy.....	78
Impact and results.....	80
Lessons learned and future aims	80
Conclusion.....	80

Case study 5: UK Health sector – Introducing information tools to capture corporate memory.....	83
Overview	83
The problem of corporate memory.....	83
Capturing corporate memory.....	84
Retrieving corporate memories.....	85
Raising project performance	85
Learning lessons	86
Conclusion.....	86
Part Three: Appendices	
Appendix 1: Information risk and control assessment tool.....	91
Form 1: SIRD authorisation form.....	91
Form 2: Information risk and control assessment register form.....	92
Form 3: IRCA action plan form	93
Appendix 2: Information risk matrix.....	95
Risk scoring	95
Risk prioritisation and action.....	96
Appendix 3: Sample information risk management policy.....	97
Index	101

Executive summary

EVERY ORGANISATION faces a range of threats including information risks. From healthcare providers to multinational companies, all organisations are seeking to deliver value, vision and objectives in the face of threats and risks.

Risk, just like death and taxes, exists as an inescapable part of everyday life. Most people view risk in purely pessimistic terms. But there are two sides to risk: positive and negative. Organisations that continue to improve and succeed have learnt to consider threats and take intelligent risks, as 'without risk there is no reward'.

Information is a key asset for any organisation but is itself loaded with potential risk, threat and opportunity. The potential for loss, destruction or theft of key business information can lead to significant damage to even the largest global organisation. By contrast, the protection of key information, such as new designs, can allow an organisation to innovate and take positive risks to increase business.

The economic uncertainty of recent times has created enormous risks for organisations. Specifically, organisations are facing severe budget cuts and are seeking ways to deliver more for less, rationalise processes and weed out inefficiencies to cut costs and boost productivity. A major asset or potential overhead for organisations relates to how information is managed and valued. The value of information relates directly to an organisation's approach to information risk management. Indeed, the

approach to this type of risk is the defining strategy for all organisations.

The strategic, operational and financial risks arising from myriad information management programmes are significant and often poorly managed. In these straitened times how can organisations adapt to an array of information risks that could impact on them, ultimately leading to a firm's demise? Should firms risk cuts now to survive over the longer term?

Information risk does not yet have a high profile. This is evident in many organisations where a major problem is that staff are continually drowning in data, yet starved of information. This presents both a cost and a major risk to the organisation. The challenge over the next five years for information professionals will be how to embed information risk management (IRM) into organisational culture.

The integrated information risk management framework has been developed following extensive consultation across the United Kingdom public and private sectors. It is a flexible method that provides a complete toolkit for organisations to scan, assess and develop risks into business intelligence. By introducing the strategic information risk management processes defined within this framework, the value of information can be protected and even raised whilst reducing threats and vulnerabilities.

This report focuses on how to integrate an information risk management approach with corporate information and knowledge

strategies to reduce costs and deliver value. It draws on leading practices adopted by a variety of public and private sector organisations and includes comparative analysis of best practices.

This publication shows information professionals how to develop risk strategies that integrate planning and policy making to manage and mitigate risks arising from legal compliance, technology projects and change initiatives.

Chapter 1 introduces key concepts, principles and issues relating to IRM.

Chapter 2 looks at the IRM improvement techniques. This chapter brings together the key processes, techniques and information products required to deliver improved IRM.

Chapter 3 explores the first improvement technique, information scanning. This reviews improvements to information gathering and processing for better business intelligence.

Chapter 4 focuses on the information assessment improvement technique, which takes the products of the scanning process and builds them into a corporate development process.

Chapter 5 begins with an overview of the information and intelligence development process. It shows how to use key tools to deliver improvements and monitor performance.

Chapter 6 reviews methods for information risk management improvement capitalisation and the valuation of information assets.

Chapter 7 considers corporate governance and performance management for information professionals adopting improvements in IRM.

Chapter 8 looks at the integrated IRM framework within organisations and the future issues for information professionals working in this sphere.

Part Two focuses on five case studies of organisations, both public and private, which

have undertaken IRM initiatives. The case studies provide key learnings and examples of best practice to help readers adapt and introduce new practices into their organisations.

The appendices in Part Three provide useful tools and templates for implementing information risk management in your organisation.

A recession is a great time to begin to think differently. A new approach to information risk management can underpin a range of improvement initiatives and free organisations from threats and reduce vulnerabilities during challenging economic circumstances.

About the author

Robin Smith is currently head of information governance for Northampton General Hospital. He has worked extensively in the UK police service as a senior information management change manager.

Robin was formerly marketing director of the Records Management Society UK and will shortly publish his first book, *Legacy information management: strategies for optimisation*.

Robin is currently developing innovative approaches to legacy content management with a focus on e-mail optimisation and information systems integration.