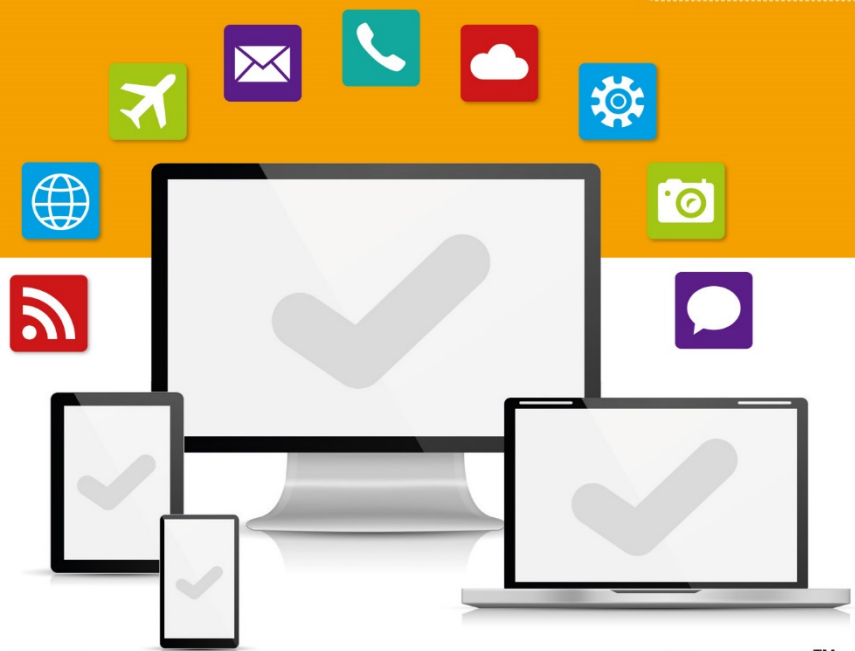
FUNDAMENTALS OF INFORMATION RISK MANAGEMENT AUDITING

An introduction for managers and auditors

Christopher Wright



Information Security buzz

itgp™

Fundamentals of Information Risk Management Auditing

An Introduction for Managers and Auditors

Christopher Wright

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely
Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

First published in the United Kingdom in 2016
by IT Governance Publishing.
ISBN 978-1-84928-815-6

FOREWORD

It's often said that we live in the 'Information Age'. When we consider our lives and how important information has become over the last 20 or so years, it is amazing. Every decision we make is based on information – be it our choice of holiday, career, new car, or where to live. Thanks to social networking, we know more about what our friends, family and associates are doing right now (often more than we would like to know!). Events on the far side of the world are streamed to us in real time. We can search for answers to the most obscure questions imaginable – even during the quiz at our local pubs. We can watch movies, read books from a library of many works, check out our contacts, and review the news and share prices – all from our telephones and mobile devices – almost anywhere in the world. New businesses are thriving in sectors unimaginable 20 or so years ago – social networking, sale of content and knowledge, online shopping and take-away food, to name but a few. Even well-established businesses have changed the way they operate and interact with their customers.

These changes are historic, comparable to the impact of exploration of the New World in the late middle ages, or indeed the Industrial Revolution. There are risks – we are all aware of the scares around loss of personal and highly sensitive data by large organisations, disasters impacting data centres, etc.

We all need to be aware of these risks and adapt strategies and processes which will enable us to reduce the likelihood and impact of these risks to acceptable levels.

PREFACE

At my age I don't remember much about my school days. But I do have a very vivid memory of being shown a 35 mm film (yes it was a long time ago) called GIGO – 'Garbage in Garbage Out'. I watched it again recently on YouTube and was struck not only by what had changed so dramatically (no more ticker tape and punched cards) – but also by what had not changed. The risk of programming errors, security and need to change business processes are the same today as they were in 1969 when the film was made. Added to that, we have new risks and challenges with viruses, hackers and advanced persistent threats (APTs), to name a few. The modern information risk manager and auditor needs an appreciation of the whole realm of information risk and governance, in addition to a detailed understanding of their own specialist fields.

I also remember running training in the early 1990s when we stated that by 2002 there would be no computer audit/information risk management (IRM) specialists – all auditors and consultants would have the necessary skills to undertake the work themselves and so specialists would not be required. Thankfully (for me) this has not been the case. The need for IRM specialists/auditors is now greater than ever, as threats have become more complex (e.g. APTs, cyber crime and terrorism). At the same time, the traditional threats still remain and are compounded by general ignorance and naivety of the risks. It is however true that all auditors need an appreciation of the basic information risks facing their organisations and how these can be mitigated.

The aim of this book is to provide insight and guidance for those considering a career in information risk management, and also to provide an introduction for non-specialists. It has been written in four main parts:

I. What is risk and why is it important?
   This provides an introduction to general risk management and introduces information risk.

II. Introduction to general IS and management risks
   This gives an overview of general IS controls and the controls over the operation and management of IS. It also considers risks and controls for confidentiality, integrity and availability of information.

III. Introduction to application controls
   This introduces the concepts of application controls, the controls built into systems to ensure that they process data accurately and completely.

IV. Life as an information risk management specialist/ auditor
   This provides a guide for those considering, or undergoing, a career in information risk management.

Each chapter contains an overview of the risks and controls that you may encounter when performing an audit of information risk, together with a suggested approach. I have based this approach on risks and controls rather than providing a detailed list of specific questions – given the variety of organisations and technologies in use, I find such questions of very limited benefit unless they are used effectively.

This book is not intended to provide an in-depth analysis – however, there are references to other sources. I hope you find the book helpful, informative and entertaining. Happy auditing.

ABOUT THE AUTHOR

A qualified accountant, Certified Information Systems Auditor and Certified ScrumMaster™, Chris has over 30 years' experience of providing financial and IT advisory and risk management services. He worked for 16 years at KPMG where he managed a number of major IS audit and risk assignments. These included a number of project risk and business control reviews. He was head of information risk training in the UK and also ran training courses overseas including India and throughout mainland Europe. He has worked in a wide range of industry sectors including oil and gas, public sector, aviation and travel.

For the past eight years he has been an independent consultant specialising in financial, SOX and operational controls for major ERP implementations, mainly at oil and gas enterprises.

He is an international speaker and trainer on Agile audit and governance and has published two other titles for ITGP:

1. *Agile Governance and Audit* (2014)
2. *Reviewing IT in Due Diligence* (2015)

ACKNOWLEDGEMENTS

Throughout my career I have been blessed with meeting many people who have extended my knowledge and skills – even though in some cases this was as a result of the mistakes that we made together, rather than anything intentional. They were always patient and keen to help me develop my skills – some becoming lasting friends over many years.

I also greatly appreciate the support and advice provided by my friends and former colleagues in the production of this book. In particular, the guidance and support from Diane Hill, Colin Bezant, Scott Nicholls, Mike Hughes, Jackie Price and Manoj Shah – and not forgetting of course the patience and guidance of my wife, Amanda.

As always, I have received great patience and support from the publisher, ITGP, particularly from Vicki Utting and Sophie Sayer. Also to their reviewers, Antonio Velasco and Maarten Souw, for their valuable advice and guidance.

CONTENTS

PART I: WHAT IS RISK AND WHY IS IT IMPORTANT?

CHAPTER 1: RISKS AND CONTROLS

Overview

Before considering information risk, we need to understand the basic concepts of risks and how they can be managed. This will put the management of specific IT risks into context and also improve our communication with other risk management professionals. Following financial and other business scandals and crises, there has been an increased focus on risk – a whole industry has been created around the Sarbanes-Oxley Act, impacting US based companies. It has also become an area for academics and standard setters.

In this chapter we will consider:

- What is risk?
- Management of risk
  - Risk awareness and identification
  - Assessing and monitoring risk
  - Responding to risk.

At the end of the chapter there is a summary of the key points.

What is risk?

Risks are all around us. They are part of everyday life – whether we are walking to the shops or climbing Mount Everest. When the first caveman left the shelter of the cave there was a risk of accident, or wild animals, or even other cavemen. We deal with risks all of the time, often

without even thinking about them. Some are small – some are huge. There is a saying where I come from that roughly translates as "He who makes no mistakes makes nothing". In other words, without risk there can be no endeavour. Columbus could just have said – "But I might fall off the edge of the world, or die of starvation, or get attacked by wild animals or natives – I think I will stay at home". But instead he weighed the risks, took reasonable steps to reduce them and went anyway. The same could be said of the early IT pioneers. They could have simply decided the risks were too great and just not bothered to invent computers, the Internet, etc. Apple, Facebook and Google are all examples of global IT-based organisations founded by a few people willing to take managed risks.

Risks are not certainties. They may not happen. But if they do, they will have consequences. Take space flight for example, if the early pioneers had sat down and listed all of the things that could go wrong, no one would have left Earth's orbit. Instead, they took a more pragmatic approach, reducing risk where they could, based on their existing knowledge, and then adapting as they learnt lessons and became aware of the major risks.

We could say all new exploration stops (event) because of a fear of risk (trigger) and therefore we do not achieve new inventions or developments (consequence).

Management of risk

Risk management is big business. Consider, for example, the number and size of security companies, health and safety, police, fire, insurance, military, audit and of course information risk specialists. When you look at each of

these there are a number of common themes in how they deal with risk:

- Identify threats thereby raising awareness of risk and its consequences.
- Have frameworks for assessing risk.
- Have response mechanisms for reducing risk to an acceptable level.
- Establish monitoring arrangements to see if the risk impacts, or if new risks arise.

Risk identification and awareness

Risk awareness comes from experience and learning. Whenever there is a major disaster we have an opportunity to learn and take different future actions. For example, the sinking of the Titanic led to an awareness of the need for more lifeboats on ships. The discovery that the wrong shaped windows on the Comet aircraft led to metal fatigue when the airframe was under stress, led to fewer air crash incidents.

We all have a different appetite for the risks we are willing to take. If this were not the case, there would be no gambling – as this depends on odds being set based on each of our perceptions of risk and reward. If we all felt the same, we may all want to back the same horse or dog. Or conversely, we could live in a world where everyone gambles recklessly, undertakes dangerous activities without any safety devices, or disappears up the Amazon basin!

In practice, we all have our own level of risk appetite. This will be based on personal experience, our life/financial

situation, etc. Unlike risk likelihood/probability and impact it is difficult, if not impossible, to place a metric onto risk appetite. It is a very subjective matter and is not fixed, as it can change as a person or an organisation matures. The risk appetite for an entity will largely be defined from the Board and communicated down. If it is not, the organisation may be taking too little or too much risk to achieve the objectives set by management. Management need to set strategic, financial and operational parameters which provide the decision makers within the organisation with a good steer as to how much risk is acceptable. In addition to experience and situation, external factors will also influence appetite, for example the fiscal and regulatory/ compliance framework the entity operates in, and economic and political factors, will all have an influence. Audit has an important role in challenging management's risk appetite – acting as a check and balance. Similarly, IT audit holds IT management (and the business) to account, in its use of IT.

Documenting risks

There are a number of ways we can state risks. The one I prefer and will use throughout this book, is that something could happen due to an incident that has implications, or:

<Event> <trigger> <consequence>

For example, there is a risk:

- I may get an electric shock ('event') if I put a metal screwdriver into a power socket ('trigger') and so I will die ('consequence'); or

- a hacker could gain access to my bank account ('event') because I am not careful with my passwords ('trigger') and so I will lose most of my savings ('consequence'); or
- I may have a virus on my computer ('event'), if I switch off my antivirus software ('trigger'), and so I could lose my important data and files ('consequence').

Whilst being simple, this approach provides consistency and clarity – the reader can immediately see why the risk is important. I often see risks written as statements, such as:

- Lose customers
- Get prosecuted for health and safety
- Get fined for breaking data protection.

In each of the above examples, the definition is too general; it does not tell why this event may occur, the specific nature of the event, or what will happen as a result. The risk definition should answer the questions 'How?', 'Why?', 'So What?'. It should be brief, no more than a couple of sentences. It should, however, provide enough information to enable analysis and evaluation of the risk.

Some methodologies consider risk as positive as well as negative – i.e. a risk can be an opportunity as well as a threat. When we look at this format <event> <trigger> <consequence> we could apply it to opportunities as well as risks. For example, "If I bet on the 3.30 pm race, the horse I back may win, therefore I will be able to buy myself a treat". Just like risks, there is uncertainty of outcome but we are expressing what could happen.

Within IT projects, risks can be positive as well as negative. For example, if we launch a new website there

is a risk that it may be more popular than we expected, leading to a quick return on investment/achievement of business benefits. This may lead to a need to move to the next phase of the website faster than originally intended.

Assessing and monitoring risk

The first consideration is what risks are relevant to the situation being considered. This sounds obvious but I have reviewed many risk frameworks that have simply looked at the wrong risks. The risk may be real but might not have any consequence or specific impact on what we are trying to achieve. For example – the end of the world as we know it could be a real risk. But I don't really need to consider this if I am trying to perform a risk assessment for going to the shops, or launching a new product, or embarking on a new software project.

Risk assessments may be performed at a number of different levels. The Board, or top management of the organisation, for example, may be interested in strategic risks. The finance department will be mainly interested in financial risks. There may be different risks for different operating divisions of the business. There may also be a need to perform a risk assessment for a new project or product being considered for sale. The following techniques can be used in all of these situations.

We all have different perceptions of risk, depending on our experiences and how brave we are. When reviewing risks for an ongoing activity or new endeavour, most organisations will perform a brainstorming workshop – bringing together the main impacted parties. As a risk

management professional, you may be called upon to facilitate at such an event. The aim is to allow the discussion of potential risks. It is a cliché but at this stage nothing should be ruled in or out. The facilitator should document all suggestions – no matter how outrageous, as this idea may be a thread leading to a real risk. The best facilitation I ever did was in Flemish and I don't speak a word of it! There was a risk workshop for the audit of an airline – the workshop was a team of Flemish speakers, some of whom found English difficult to work in. So I would introduce a topic and then stand back and let discussion continue. When it went quiet, I asked someone to translate their findings into English, I wrote it down and moved on. The reason it went so well was as a facilitator I could not over influence what was being discussed.

When the list of risks is complete, an assessment of the suggestions can be made. The usual way for a risk assessment is to consider categorisation of the risk, its likelihood and the extent of the potential impact if it does occur. Most organisations will have their own definitions for each of these. I have a given a general overview below.

Categorisation

The common categorisations of risks for organisations are:

- Financial/financial reporting
- Fraud or financial irregularity
- Health and safety
- Going concern/business continuity
- Reputation risk
- Customer impact

- Regulatory or compliance risk
- Strategic risks
- IT and technological risks.

The extent and appetite for each of these risks will depend on the individual organisation. For example, financial reporting risk is very high on the agenda of companies registered on the US stock exchanges, as they need to comply with the Sarbanes-Oxley Act for control over financial reporting. There is also a need for monitoring to ensure that this appetite is not being breached. The following diagram illustrates the top-down direction of the definition and communication of appetite and the reverse bottom-up direction of monitoring.

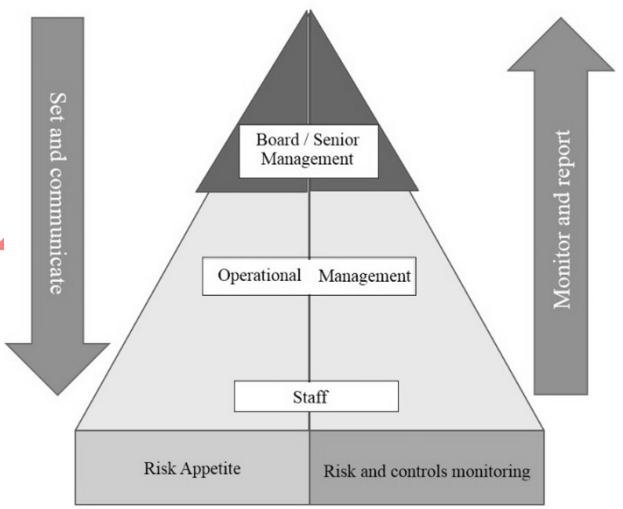


Figure 1: Risk appetite and risk monitoring within an organisation

Likelihood

We need to focus on risks leading to events that are likely to happen. Many organisations have their own categorisations for this. I favour something like Table 1.

Table 1: Assessment of risk likelihood

	Likelihood	Description	Example
5	Almost Certain	Very likely as the event is expected to happen.	We will get rain during winter in London.
4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence.	Snow during winter in London.
3	Possible	The event might occur at some time as there is a history of casual occurrence.	1 in 100 years flood in London.
2	Unlikely	Not expected to occur but there's a slight possibility it may.	Earthquake in London.
1	Rare	Could happen, but probably never will, unless we have very exceptional circumstances.	Volcanic eruption in London.

There is a danger that people will always choose the middle option i.e. 'possible' in the above. To get around this, some organisations use an even, rather than odd,

number of categories. For example, if we use six categories it forces a decision for a middle grade between three or four, forcing the assessor to decide between 'bad/medium' and 'medium/good'.

If the likelihood is low, it is unlikely to be cost effective to mitigate the risk – the cost of mitigation would be higher than any benefits from resolving it.

Impact

The assessment of impact will depend on the category of risk being considered and the risk appetite of the organisation or business unit. For example, financial risk can be assessed in terms of monetary values, health and safety in terms of incidents/level of injury sustained, etc.

Table 2: Assessment of risk impact

	Description	Financial Impact	Health and Safety
5	Catastrophic	Above £10M	Fatalities or permanent disability or ill-health
4	Major	£5M to £10M	Single death and/or long-term illness or multiple serious injuries
3	Modest	£2M to £5M	Injury; possible hospitalisation and numerous days lost
2	Minor	£300,000 to £2M; not covered by insurance	Minor injury; medical treatment and some days lost
1	Insignificant	Less than £300,000	No or only minor personal injury; first aid needed but no days lost

Unlike the likelihood category, we are able to attach specific values to each category. There is still a highly subjective element in assessing the category for each likely event, but it should be possible to rationalise and document the assumptions that have been made in making the assessment.

Risk heat maps

Having agreed values for the likelihood and impact of each risk, a common way of displaying and comparing the results is to create a matrix in the form of a risk heat map.

Impact	5	High impact/low likelihood	High impact and high likelihood
	1	Low impact and low likelihood	Low impact/high likelihood
		1	5
		Likelihood	

Figure 2: Risk heat map template

Any risks in the top right hand corner will need to be treated as priority. The aim is to introduce mitigations to reduce either the impact or the likelihood of the risk occurring. Typically, organisations will consider their top ten risks and review these on a regular basis to see if there has been any substantial change in risk profile. It is important for the auditor to understand and challenge an organisation's perception of risk and their risk appetite. When an organisation or a project fails, or suffers a major incident, it is often because of a risk that was known about but the likelihood and impact had been underestimated.

One example of this is the risk of mountaineering vs skiing. One of these activities seems inherently more risky than the other. However, the cost of insurance is the same for both – as the chance of an injury or loss of property when skiing is higher than the chance of injury or loss of property when mountaineering, but the impact of the injury/loss is likely to be higher when mountaineering. Our perception is altered by comparing mental/video images of climbers trapped on Mount Everest with advertisements of smiling people on gentle snow-covered slopes.

In the same way, IT organisations are often well protected against the obvious threats but not against those from new/emerging risks and technologies.

Controlling risk

Our human evolution, and indeed our own personal childhood and development, have taught us how to respond to risk. We can run away or avoid a threat ('flight') or alternatively we can conquer the risk by finding a solution ('fight'). By choosing a career in information risk management I have resolved to:

- make management aware of the information risks that are too big to resolve based on our current tools and so need to be avoided.
- help to develop controls and other mitigations which will reduce and monitor risks so that they can be overcome and benefits can be achieved for the organisations we work for.

However, there may still be occasions where the likelihood or potential impact is so small that we choose to 'run away' from the risk, i.e. accept or ignore it.

The level of mitigation needs to be appropriate but not too onerous. I was once asked how much a particular local authority should spend on their disaster recovery arrangements. My answer was that it depended on whether or not they had an incident. If there was an incident, I said they would probably wish they had spent more – if not, they would probably have wished they had spent less. It's the same with any insurance premium. The estimate of

likelihood gives an indication, and together with impact, is useful to help assess how much mitigation is required.

There are various ways to remember how to manage risks. They all follow the same terms and one I use is 'TRAIN':

Table 3: Risk treatments

Transfer	Move responsibility to a third party – for example, outsource security, take out insurance, have a disaster recovery service provider.
Reduce	Take pro-active actions to reduce the likelihood or impact. For example, reduce or cease the activity.
Avoid	Avoid the activity so that the risk will not affect us.
Ignore	Accept the risk and continue with the activity. May still include some monitoring to ensure that the risk profile does not change.
Negate (removal)	Changing some aspect of the activity – for example, scope, procurement route, supplier, or sequence of activities. This could include, for example, centralising an activity.

Each of these activities, with the exception of 'ignore', have cost/resource implications and these need to be considered in terms of the cost benefit for the reduction in risk that they could achieve.

If organisations can handle risk, it can give them a competitive advantage over other similar organisations that cannot work at the same level of risk. This is particularly true in information risk management, for example, the development of techniques to authenticate

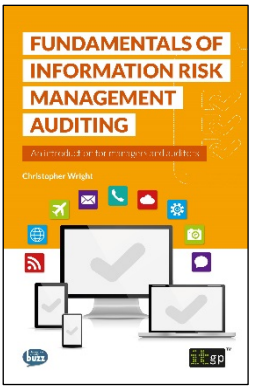
customers has enabled online banking and other commerce whilst not increasing risk.

The key to successful control of risk is to ensure that there is clear ownership and accountability. In many audits I have found it very difficult to identify a specific risk owner who is accountable in this way. A good starting point is to consider the following questions:

- Who would be accountable if the risk became a real business issue?
- Is this clearly understood and communicated?
- Is the control owner fully aware of this responsibility?
- Who would suffer the most?

Summary

Risk and uncertainty about future events is a part of everyday life and in order to thrive and progress we need to be able to handle it in a way that is sensible and not excessive. This depends on the individual or organisation's risk appetite. We need to identify, document (<event> <trigger> <consequence>), assess and manage risks appropriately, particularly those with high potential impact or likelihood. This applies to both positive and negative risks. In order to mitigate and control risks they should be assigned to risk owners.



"It is good to have such a useful guide for our chosen profession, Information Risk Management and auditing."

"This book will be particularly useful for anyone involved in the audit of information security and risk in all organizations that have related issues and concerns."

Buy your copy today

www.itgovernance.co.uk/shop/product/fundamentals-of-information-risk-management-auditing

www.itgovernance.eu/shop/product/fundamentals-of-information-risk-management-auditing

www.itgovernanceusa.com/shop/product/fundamentals-of-information-risk-management-auditing

www.itgovernance.asia/shop/product/fundamentals-of-information-risk-management-auditing

www.itgovernancesa.co.za/p-1044-fundamentals-of-information-risk-management-auditing.aspx