Connect › Support › Advance

The Institute of Internal Auditors Australia

White Paper

Agile Risk Management

Updated 2023

Level 5, 580 George Street, Sydney NSW 2000 | PO Box A2311, Sydney South NSW 1235
T +61 2 9267 9155 **F** +61 2 9264 9240 **E** enquiry@iia.org.au **www.iia.org.au**

Agile Risk Management

Contents

Background	2
- Purpose	2
- Background	2
Discussion	2
- Issue	2
- History	2
- Discussion	2
Conclusion	7
- Summary	7
- Conclusion	8
Bibliography and References	8
Purpose of White Papers	8
Author's Biography	8
About the Institute of Internal Auditors–Australia	8
Copyright	9
Disclaimer	9

Background

Purpose

This White Paper examines what risk management could potentially do better and contrasts the concepts of:

- Traditional risk management – built from the risk management common body of knowledge using traditional methods but over-engineered, slow to react and not dynamic.
- Agile risk management – adopting new ways of working for risk management practitioners to foster stakeholder engagement and collaboration through use of dynamic methods.

Background

Getting people interested in the concept of risk management is difficult, partly because it is not seen as core business and so does not get the attention it should. And also because in most cases it is:

- Not dynamic.
- Slow to adapt.
- Not showing the up to the minute risk situation.
- Not horizon focused.
- Using outdated methods.

While risk management should be a dynamic activity that can quickly pivot to changing circumstances, in practice it seldom is.

Discussion

Issue

The issue to be discussed is how can risk management be a dynamic activity that is embraced by stakeholders?

History

Formal risk management concepts evolved over the past 30 years, with standards of practice first issued in 1995 in Australia – though best known for the 2004 Australian / New Zealand standard and 2009 (now 2018) international ISO standard.

Risk management governance sits in the 2nd line of the '3 lines model'. Its job is to make sure 1st line business activities are effectively risk managed. Many 2nd line risk management functions see themselves as discrete functions and do not seem to recognise the fact that their effectiveness is dependent upon the risk maturity of the 1st line. The '3 lines model' defines the job of the 1st line is to manage risk, with the 2nd line an enabler and adviser. Risk management (2nd line) would not exist without the 1st line.

Discussion

What is Risk Management?

Risk is the effect of uncertainty on objectives, with:

- An effect being a deviation from the expected which can:
  - Be positive, negative or both.
  - Address, create or result in opportunities and threats.
- Risk is usually expressed in terms of:
  - Risk sources.
  - Potential events.
  - Their impact (consequence).
  - The probability (likelihood) of experiencing the impact.

An organisation will normally assess risks against a pre-determined appetite towards risk taking.

Risk management comprises co-ordinated activities to direct and control an organisation with regard to risks – this requires co-ordinated and economical application of resources to

Agile Risk Management

determine the level of risk treatment required to:

- Minimise, monitor, and control the probability or impact of unforeseen events.
- Maximise the realisation of opportunities.

What are Traditional Risk Management Limitations?

Some risk management characteristics do not have the desired effect of encouraging or embedding risk management practice within organisations and often run counter to this objective, in particular:

- Voluminous frameworks and documentation – there are often multiple documents that contain similar information such as policy, procedure, framework, risk matrix, risk management plans, risk registers, etc.
- Risk management jargon for example risk culture, risk universe, risk appetite, risk tolerance, risk register, inherent risk, residual risk, etc. Facilitate a risk workshop in a hospital and see the reaction you get when mentioning 'risk treatments'.
- Tedious risk workshops that seem to take hours or even days of people's lives.
- The difficulty people have identifying and assessing inherent risk (risk without controls applied) – they find it almost impossible to assess the risk without considering the controls already in place.
- Control effectiveness assessments not done well, if done at all.
- Many people when identifying mitigating actions to help further reduce residual risk (risk after controls applied) come up with something that is not easily measured and where the link to the risk can be tenuous.
- Strategic and operational risks mixed together.
- Periodic risk reporting where risks and ratings never seem to change over time.
- Lengthy and complex spreadsheet reports that cannot be read unless printed on A3 paper.
- Above all, getting people interested in the concept of risk management – this manifests itself in a general level of disinterest that makes the job of a risk management practitioner more difficult than it need be – this is an inability for risk management to articulate to stakeholders 'what's in it for me?'.

What is Agile Risk Management?

When we talk about agile risk management, we are focusing on two things:

- A nimble risk management response and approach to the changing dynamics in the organisation's risk management landscape to provide a timely risk management service to the board (or equivalent governing body), audit committee and senior management.
- Leveraging agile project management techniques such as sprints to split the risk management service into manageable chunks, enabling risk management practitioners and stakeholders to collaboratively work together to stay timely and quickly update the risk management focus.

The term 'agile risk management' suggests risk management should practice:

Engagement	Risk management practitioners actively engaging with people to manage their risks.
Collaboration	Managing risks through team effort between 1st line business activities and 2nd line risk management.
Dynamic	Recognising there is constant change in organisations and risk management needs to be continually re-evaluating the risk environment.
Adaptable	Rapid adjustment to new risk environment conditions as they emerge.
Timely	Risk reports contain the latest up to the minute risk situation.
Horizon Focus	Focusing on the risk horizon to provide early warning of potential and emerging risks.
New Ways of Working	Introducing innovative risk management methods, documentation and reporting formats.

Agile Risk Management

Agile versus Traditional Risk Management

Technique	Agile Risk Management	Traditional Risk Management
Framework and Documentation		
Plain language		
Multiple documents		
Single or small number of documents		
Complex risk registers		
Simple risk registers		
Primary Focus		
Strategic		
Operational		
Projects and major business initiatives		
Information Gathering		
Environmental scan		
Industry trends		
Regulator reports		
SWOT analysis		
Research		
Interviews		
Focus groups		
Workshops		
Workshops with blind voting		
Kanban LEAN approach		
Surveys		
60 second surveys		
Polls		
Risk scenario analysis		
Quantitative risk assessment		
Monitoring and Updates		
Automated risk management systems		
Email		
Interviews		
Workshops		
Surveys		
60 second surveys		
Polls		
Reporting		
Microsoft Word or Excel reports		
Microsoft Powerpoint reports		
Dashboard reports (multiple pages)		
Dashboard reports (one-page)		
Oversight		
Board and audit committee		
Corporate executive		
Internal audit		

High Focus	Moderate Focus	Low Focus

The information below aligns with the various risk management techniques in the table above and provides commentary on their application.

Framework and Documentation

Plain language

Language used in the risk management process should be readily understandable by people without knowledge of risk management.

Multiple documents

People will rarely read multiple documents relating to the same topic, and especially if they are lengthy and comprise many pages, so the effort risk management practitioners put into their frameworks and documentation can be largely wasted effort.

Single or small number of documents

There is a much better chance of documents being read and understood if they comprise few pages and are short, sharp and to the point.

Complex risk register

Risk registers containing large amounts of data covering a wide range of details of can be difficult to read and be seen as over-engineered – all the data may seem important to a risk management practitioner but is unlikely to be seen in the same light by the reader.

Agile Risk Management

Simple risk registers

A risk register in a simple and easy to read format will get more focused attention than a complex version.

Primary Focus

Strategic

Strategic risks are those that directly relate to corporate plans being successfully implemented and which can get in the way of an organisation achieving its objectives – these are where most risk management focus should occur.

Operational

While important, operational level risks are unlikely to have the same impact potential as the strategic level risks – which is why strategic risks should have the greatest focus. Operational risk assessments and risk registers across the various business units or operational activities can contribute to strategic risk identification and informed business unit planning, but the process does not necessarily need to take-up significant time and effort.

Projects and major business initiatives

Projects and major business initiatives are usually among the riskiest things happening in an organisation, but often do not receive the level of risk management attention they should.

Information Gathering

Environmental scan

An environmental scan is a systematic process used in strategic planning to survey and interpret relevant data to identify opportunities and threats that could influence future decisions – they can be useful to see what is happening in the environment surrounding an organisation. As an example, the emergence of ESG (Environmental, Social and Governance) reporting by competitors could promote strategic decisions to implement ESG in your organisation.

Industry trends

Industry trends are the general direction in which something is developing or changing – it can be useful to see what is happening in the organisation's industry, similar organisations and competitors to consider what lessons and potential impacts there may be for your organisation. For example global issues that have arisen with wage theft, cyber-crime, and modern slavery in supply chains. Conversely, there are likely to be opportunities to pursue further reduction of red tape imposed by governments, regulators or internally within the organisation.

Regulator reports

There are many sources of regulator reports, with some covering industry groups and some specific to individual organisations. Organisations should review regulator reports to see whether the lessons contained in them may be applicable to their organisation. For example (a) a regulator report of maladministration in a local government council should result in at least a self-assessment by other councils (b) a national regulator identified thousands of cash transactions above a legislated value and imposed a $700 million fine for serious breaches of anti-money laundering and counter-terrorism financing laws – this should automatically result in an expert assessment at other financial institutions.

SWOT analysis

SWOT analysis is a 'meeting of the minds' in an organisation to mutually decide what Strengths / Weaknesses / Opportunities / Threats the organisation faces.

Research

It is useful to monitor emerging and prominent risks through research and reporting undertaken by thought leaders across the world. For example, each year the European Confederation of Institutes of Internal Auditors (ECIIA) issue a 'Risks in Focus' report to identify and prioritise the top five risks that organisations face, together with the multi-year trend – the report is freely available on their website.

Interviews

One-on-one interviews can be a useful method to gather information that can then be collated to show consensus areas in relation to risk management. The downside is it takes a lot of time and is usually done at significant intervals, often annually, and so could not be considered to be particularly timely.

Focus groups

A focus group is a research technique where a small group of people meet with a facilitator to discuss a specific topic to better understand the group's perceptions and reactions to particular questions or scenarios.

Agile Risk Management

Workshops

A workshop is a facilitated session that brings a group of stakeholders and specialists together to collaborate, define and agree on a deliverable. They can be an effective information gathering tool but need to be well-planned and well-executed to succeed – they are extremely time-consuming and can be dominated by opinionated individuals.

Workshops with blind voting

Same as 'Workshops' above – The blind voting aspect is a means of agreeing endorsed outcomes using voting technology that does not identify who cast votes.

Kanban LEAN approach

A Kanban LEAN approach seeks to promote a continuous flow of delivery rather than one delivery at the end. This may include leveraging agile project management techniques such as sprints to split the risk management service into manageable chunks, enabling risk management practitioners and stakeholders to work together to quickly update the risk management focus.

Surveys

Surveys or questionnaires contain multiple questions and can be a method to collect data from a range of people in a short time. They need to be targeted and done well with few questions and limited request for free-text commentary. Some people prefer surveys where responses are de-identified and anonymity is preserved. Surveys need to be useful to potential respondents, be brief to encourage responses, take little time to complete, not ask for much in the way of free-text commentary, and use modern technology to be successful – if a person has to download a Microsoft Excel file it is less likely they will respond. Respondents are more likely to respond (and respond quickly) through a technology-based survey solution with an easy-to-use tool such as Survey Monkey.

60 second surveys

A short, sharp and targeted 60 second survey can be an effective way to quickly get people's thoughts on risks.

Polls

On-line polls usually contain a single question and can be an effective way to obtain risk perceptions from a range of stakeholders. They are 'short and sharp' and their brevity means more people are likely to respond.

Risk scenario analysis

Risk scenario analysis leverages adverse impacts within the business or across the globe to take a deep dive. For example, you might hear that a hospital back-up generator failed when temperatures exceeded a maximum level – what would happen if that occurred in your business? What would the impact be? How would the impact be presented or minimised? What strategic investment might need to be made?

Quantitative risk assessment

A systematic approach to measure (quantify) risks associated with a process – especially useful when the monetary value of a risk can be quantified.

Monitoring and Updates

Automated risk management systems

Automated risk management systems can be a good way to get consistency throughout an organisation when it comes to risk management. It can also be useful for regular monitoring of risks and obtaining updates from risk owners. Use of risk management systems is usually dependent on organisation size and may not be cost-effective for smaller organisations.

Email

Using email may not be the best method to request risk updates. It generally relies on people to download and later upload updated documents which can be time-consuming and annoying.

Interviews

One-on-one interviews are a method to get together with risk owners to review risks and obtain updates on progress to implement risk mitigation actions – it takes a lot of time to get to a range of people across an organisation and is not generally timely as they are done at periodic intervals.

Workshops

Same as 'Workshops' above – A facilitated workshop approach can be used to obtain updates on progress to implement risk mitigation actions. They are time consuming activities and probably best left to areas of greatest risk to get optimum results from the time invested in a workshop.

Surveys

Same as 'Surveys' above – Surveys or questionnaires can be a method to obtain risk updates from a range of people in a short time.

Agile Risk Management

60 second surveys

Same as '60 second survey' above – Can be an effective way to quickly get people's thoughts on the current situation around risks.

Polls

Same as 'Polls' above – Can be an effective way to obtain risk updates from a range of stakeholders.

Reporting

Microsoft Word or Excel reports

Microsoft Word or Excel reports can fulfil a useful purpose provided they are not lengthy and are designed to attract the reader's attention – wading through pages of text is not preferred by readers. Likewise, the effort required to upload and download can be tedious and not an optimum method to encourage responses.

Microsoft Powerpoint reports

Many people prefer Microsoft PowerPoint reporting as it generally uses colour, diagrams, charts and innovative features – and importantly contains less words than other reporting tools.

Dashboard reports (multiple pages)

Dashboard reporting provides a simplified reporting format for the reader to understand risk management performance 'at a glance' – it is designed to tell the risk management story in a concise way.

Dashboard reports (one-page)

One-page dashboard reporting takes the concept of dashboard reporting further by producing an extremely concise 'report on a page' containing the 'risk management story' at a point in time.

Oversight

Board and audit committee

It is critically important the board (or equivalent governing body) and audit committee have continual review and oversight of the organisation's strategic risks – these are the things that could potentially bring the organisation undone. The strategic risks need to be updated with the latest view of what the current situation is – without this information provided in a timely way the board and audit committee are 'flying blind'. These stakeholders should also have visibility of both emerging risks and significant risks outside the risk appetite established by the board – together with periodic insights on the corporate culture.

Corporate executive

The chief executive officer and corporate executive need to build constant review of the organisation's risks into their processes. This should include time allocated at every corporate executive meeting to review and discuss the latest up-to-date assessment of the key risks facing the business – and collaboratively holding executives to account through 'peer pressure' to implement risk mitigation measures in a timely way. Ultimately, it is the organisation's response to strategic risks that should drive the strategic direction and budget-setting.

Internal audit

Internal audit should periodically review the risk management approach to provide the board (or equivalent governing body), audit committee and senior management with a view on whether the organisation is doing the right things in the right way at the right time in relation to risk management. Internal audit should be constantly working to leverage the work of risk management and to influence the quality of risk reporting.

Conclusion

Summary

For risk management practice to be successful, it needs to:

- Engage – actively engage with people to manage their risks.
- Collaborate – manage risks through team effort between 1st line business activities and 2nd line risk management.
- Be dynamic – recognise there is constant change in organisations and risk management needs to be continually re-evaluating the risk environment.
- Be adaptable – rapidly adjust to new risk environment conditions as they emerge.
- Be timely – produce risk reports containing the latest up to the minute risk situation.
- Have a horizon focus – focus on the risk horizon to provide early warning of potential and emerging risks.
- Implement new ways of working – introduce innovative risk management methods, documentation and reporting formats.

Agile Risk Management

Conclusion

Getting people interested in the concept of risk management will continue to be difficult until risk management practitioners abandon outdated methods.

Risk management will be valued when stakeholders can confidently answer 'what's in it for me?'

Bibliography and References

Bibliography and References

ISO 31000:2018 'Risk management – Guidelines'

'Enterprise Risk Management – Integrating with Strategy and Performance', COSO

The 20 Critical Questions Series 'What Directors should ask about Risk Management', IIA-Australia

Factsheet 'Risk Management', IIA-Australia

Factsheet '3 Lines Combined Assurance Model', IIA-Australia

Factsheet 'Combined Assurance', IIA-Australia

'The IIA's Three Lines Model – an update on the Three Lines of Defense', IIA Global

Purpose of White Papers

A White Paper is a report authored and peer reviewed by experienced practitioners to provide guidance on a particular subject related to governance, risk management or control. It seeks to inform readers about an issue and present ideas and options on how it might be managed. It does not necessarily represent the position or philosophy of the Institute of Internal Auditors Global and the Institute of Internal Auditors–Australia.

Author's Biography

This White Paper written by:

Andrew Cox MBA, MEC, GradDipSc, GradCertPA, DipBusAdmin, DipPubAdmin, AssDipAcctg, CertSQM, PFIIA, CIA, CISA, CFE, CGAP, CSQA, MACS Snr, MRMIA

Andrew Cox is Manager of Technical Services at the IIA-Australia, responsible for technical matters including contributions to the body of knowledge around governance, risk management and internal audit. He was previously a chief audit executive at significant organisations.

He further developed the internal audit external quality assessment process in Australia and has performed more than 300 of these in corporate and public sector organisations in Australia, Bahrain, Brunei, Kuwait, Qatar, Saudi Arabia and the United Arab Emirates.

He has made presentations on internal auditing in forums in Australia and internationally and has taught internal auditing in Australia and other countries. He co-authored the IIA-Australia publication 'Internal Audit in Australia' and co-authored 'Audit Committees – A Guide to Good Practice, 3rd edition' issued by AICD / AUASB / IIA-Australia. He contributed to 'Sawyer's Internal Auditing, 7th Edition'.

He is an independent member of a number of audit committees.

This White Paper edited by:

Lee Sullivan PMIIA, GAICD, CA, EMBA, ANZIIF (Fellow), CIP

Tracy Piscopo GradCertBus(PSM), GradCertIA, CertAL, PMIIA, PMIPAA, MAICD

About the Institute of Internal Auditors–Australia

The Institute of Internal Auditors (IIA) is the global professional association for Internal Auditors, with global headquarters in the USA and affiliated Institutes and Chapters throughout the world including Australia.

As the chief advocate of the Internal Audit profession, the IIA serves as the profession's international standard-setter, sole provider of globally accepted internal auditing certifications, and principal researcher and educator.

The IIA sets the bar for Internal Audit integrity and professionalism around the world with its 'International Professional Practices Framework' (IPPF), a collection of guidance that includes the 'International Standards for the Professional Practice of Internal Auditing' and the 'Code of Ethics'.

The IIA-Australia ensures its members and the profession as a whole are well-represented with decision-makers and influencers, and is extensively represented on a number of global committees and prominent working groups in Australia and internationally.

The IIA was established in 1941 and now has more than 200,000 members from 190 countries with hundreds of local area Chapters. Generally, members work in internal auditing, risk management, governance, internal control, information technology audit, education, and security.

Agile Risk Management

Copyright

Disclaimer