The keys to successful Integrated Risk Management

By: Gareth Byatt, Principal Consultant || Risk Insight Consulting

Date: 22nd May 2017

Summary:

This Paper discusses Integrated Risk Management in capital and asset intensive industries, and in particular how to make it effective, and the benefits that can be seen as a result. The risk profile of asset intensive industries means that they have a strong emphasis on people, safety and environmental risk as well as financial, reputational, legal, regulatory and compliance risks.

An underlying ethos of this Paper is that risk is uncertainty, and uncertainty can be positive (in the shape of opportunities) and/or negative (in the shape of threats, sometimes called risks). The management risk of risk is the management of uncertainty, and what we need to focus on is “the uncertainty that matters”.

What challenge are we trying to solve with integrated risk management?

Integrated Risk Management refers to the interconnected business activities of risk management, controls management and assurance (incorporating audit). It exists to help organisations identify, evaluate and manage the uncertainties – both threats and opportunities – that matter most to them. Integrated Risk Management must be integrated into an organisation’s DNA; it cannot be truly effective as an activity that is “external” to the regular operations of the organisation. In order for it to be integrated into the organisation’s DNA, a good culture to manage risk must exist.

When an organisational structure, environment and culture is set up properly, Integrated Risk Management can play a valuable part in addressing three inter-related challenges:

1. How to deal with uncertainty in today’s fast-changing world;
2. How to focus on the most important uncertainties to make the best decisions to manage your risk (threats and opportunities);
3. How to continuously review performance, and continuously improve your ability to thrive in uncertainty.
Insights are key to seeing clarity to risk and uncertainty

To successfully take and manage risk – in other words, to deal with uncertainty and increase predictability – we need to see good insights. Good insights about the risks we face come from having a natural curiosity and a mindset to anticipate what could happen. This mindset allows us to see signs of change early in order to do something proactive in response, and be able to navigate changing circumstances as they arise.

We are living in an information and digital age, where technology such as the Internet of Things is transforming how we manage operations in asset-intensive industries (and all other industries). These changes are fundamentally impacting how we manage risk at an operational and an enterprise / strategic level, by harnessing real-time data to optimise decision-making and achieve peak performance.

Using the right information at the right time to see insights and make the best risk-informed decisions will help you achieve competitive advantage in your dynamic and fast changing world. Changes – and events – in the external environment and internally in an organisation can quickly have far-reaching effects, which, if not anticipated and managed well, can lead to a large amount exposure and vulnerability, or lost opportunity. Seeing insights early reduces surprises and gives confidence in predicted and planned for outcomes, which maximises value to your organisation and its shareholders.

When it is done well, Integrated Risk Management overcomes a perception that may exist in some organisations that the Risk function is “not involved in running our business”. Many organisations treat risk management as a separate function to business and operations management, yet they will also describe how they manage risk in their business and on operations on a daily basis. Integrated Risk Management overcomes perceptions, or realities, that may exist of risk management being a bureaucratic, tick-the-box, low value form filling exercise which “tells us what we already know”.

This material is owned by Risk Insight Consulting. All rights reserved.
We are sailing

The sport of sailing provides an example of managing risk. You don't take part in an ocean sailing race without a plan of how to get to where you want to go, and how to anticipate and adapt to changing circumstances, which you know will happen. High performance in sailing is achieved by anticipating climate conditions, for example capitalising on downward winds and being resilient in harsh weather. You cannot wait for changes to arrive and then “go with the flow” if you want to succeed in sailing – you need to anticipate and adapt. You must be resilient so that if something unexpected occurs you can quickly respond and recover.

Seven elements of Integrated Risk Management

This paper puts forward seven connected elements that create integrated risk management (noting that it must be “integrated” into the organisation’s activities):

<table>
<thead>
<tr>
<th>Organisational factors</th>
<th>Risk fundamentals</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Organisation structure</td>
<td>4. Risk Appetite</td>
</tr>
<tr>
<td>2. Management by Objectives</td>
<td>5. Anticipate and manage risk</td>
</tr>
<tr>
<td>3. Organisation environment and culture</td>
<td>6. Risk Assurance</td>
</tr>
<tr>
<td></td>
<td>7. Continuous Improvement</td>
</tr>
</tbody>
</table>
When the three organisational factor elements are set up well, the four “risk fundamentals” elements have the foundation to provide the maximum amount of value. Whilst the focus of this paper is on asset-intensive industries, these factors can be applied to many industries and situations (including sailing). Figures 1 and 2 below describe the effect of reducing volatility that integrated risk management can have, when it is properly applied.

*Figure 1: volatility resulting from reactive risk and issues management:*

*Figure 2: predictability through proactive integrated risk management:*
Is the term “Integrated Risk Management” catching on?

The term Integrated Risk Management is becoming increasingly widespread. International standards bodies such as the ISO and COSO are stressing its importance. For example, the draft 2017 revision of ISO 31000: risk management describes the importance of integrating risk management (Figure 3):

COSO’s 2017 Enterprise Risk Management – Integrating Strategy with Performance guidance document, includes this statement in its Executive Summary (Figure 4):

---

This material is owned by Risk Insight Consulting. All rights reserved.
Embedding the seven elements of Integrated Risk Management

*Figure 5: the elements of Integrated Risk Management:*

In order to implement the seven elements of integrated risk management, two guiding principles must be consistently applied:

1. The management of risk must be woven into how the organisation and its people work, and;
2. The management of risk must not be complicated

**1. The management of risk must be woven into how the organisation and its people work**

The principle that the management of risk is part of what people do is self-evident. We all take and manage risk in our working activities every day. Integrated Risk Management means that everyone takes and manages risk using common principles and practices, and that they are ably supported and guided by a proactive Risk team that is actively working with and helping them. When this principle is followed, the sum of all risks is greater than the individual parts.

**2. The management of risk must not be complicated**

Risk practitioners must ensure that the tools and techniques they provide and train people to use, and the way that risk is managed, is kept simple. Whilst many risks are multi-faceted and some require sophisticated analysis and actions, the fundamentals of how to manage risk, regardless of its complexity, should be the same. Making the management of risk simple means ensuring that the number of risks that matter most is kept to a manageable number.
Here are a number of points to consider.

1. Your organisational structure is key

Why is it important?
Your organisational structure is a defining influence on how risk is managed by people across your organisation. Combined with the objectives setting process and the organisational and team culture that exists, it determines whether risk is managed in an integrated manner, or in silos, or not very well at all.

How does it matter?
Most medium to large sized organisations today operate as a matrix structure, with lines of business, geographies and / or product lines managing their Profit & Loss, supported by functional teams. How the organisational structure, policies and procedures and informal mechanisms are deployed across an organisation has a significant effect in how integrated your management of risk will be. For example, does information get diffused and “generalised” as it flows too slowly through reporting lines, or does it flow clearly and quickly and openly up and across horizontal lines, giving a clear “line of sight” from top to bottom which generates the right discussions about early signs of threats to treat and opportunities to be grasped.

When an organisation is structured to encourage open communication and common ways of managing risk in the everyday management of operations, Integrated Risk Management naturally occurs. If different businesses / geographies / product lines operate separately, and if their Risk team(s) is/are seen to perform separately, Integrated Risk Management is a lot harder to achieve.

What to look out for
Integrated Risk Management takes place when an organisation structure fosters lines of reporting, dotted and/or direct, through to a corporate centre and across lines of business, with business people working with their Risk team(s). People in lines of business establish a meaningful connection with their Head Office for enterprise-level risk management. Well thought through Risk Profiles (or Principle Risks), which are discussed in segment 5 (anticipate and manage risk), bind the organisation’s focus on its principle uncertainties together and ensure that the uncertainties requiring the most attention are given the focus they require.

An important indicator of how well embedded risk management is in an organisation is how the activities of the functional Risk team are undertaken, and how widespread the “basics” of risk management are. When the organisation’s Risk team is involved in business decision-making at the enterprise and operational levels, and the team is appropriately staffed with skilled people, good things happen. For example, business “gate reviews” for investments and material operational activities need due consideration of risk, against risk appetite and other elements.

In asset-intensive industries, two particular cross-functional team relationships strongly influence whether Integrated Risk Management succeeds. They are the relationships between (1) the Risk and Internal Audit teams, and (2) the Risk and Environment, Health & Safety (EH&S or similarly named) teams.
The Risk team’s interactions with all functional support teams (such as Finance, Procurement, HR etc.) are important, however their relationships with Internal Audit and EH&S are key, because asset-intensive industries focus on managing EH&S risk, and they need strong assurance practices to be overseen by Internal Audit.

The Risk and EH&S teams must share the same approach, language and methods to manage risk. In asset-intensive industries, lag indicators from operational performance can be EH&S lead indicators. Early signs of financial problems or production/project schedules starting to slip often give rise to EH&S risk. The Risk team is a valuable ally to the EH&S team to identify such “leading EH&S indicators” early so that pro-active actions can be taken according to the organisation’s appetite for risk (risk appetite is discussed in segment 4). Ideally, these two teams should sit physically next to each other to encourage cooperation. They should share the same tools and techniques to manage risk, and present a “common face” to operations and executives in management reviews, training and all other matters.

The Risk and Internal Audit teams must work closely together. Risk-based auditing unlocks a lot of value when it is performed well. It requires input by the Risk team into Internal Audit activities so that risk-based audits and appropriate reviews of the control framework and control assessments (commonly known as the second and third lines of defence) are undertaken. If Internal Audit and Risk rarely meet or do not know what each other are doing, value is lost.

2. Management by Objectives tells you what risks to focus on

Why is it important?
The management guru Peter Drucker is famously quoted as saying: “Management by Objectives works if you first know what your objectives are. 90% of the time you haven’t.”
If you do not think clearly about your objectives, the time and effort you focus on managing performance and risk will not be sufficiently focused.
All Risk standards – ISO 31000, COSO and others – stress the importance of aligning risk to objectives.

How does it matter?
Organisations exist to achieve objectives. There will always be uncertainty to achieving objectives. Good risk management is about thinking ahead and anticipating possible outcomes (good and bad), to determine how to optimise outcomes and maximise predictability. In today’s dynamic world, the need to anticipate and adapt has become more important than ever. As described in Figure 1, we want to avoid surprises and unexpected volatility in our performance. When management by objectives is done well, it ties together business management and risk management and avoids bureaucracy (such as reporting for reporting’s sake).

A key element to management by objectives is that risks must link to objectives in order for the business and risk functions to be integrated. Too often, risks that are identified and are being acted upon across an organisation do not tie back to your objectives.
Integrated Risk Management places your objectives at the heart of managing risk and uncertainty. It ensures that (1) risks are tied to objectives and (2) actions to manage risk and uncertainty are focused on having a positive impact on achieving objectives.

What to look out for
Focusing on “the uncertainty that matters” means focusing on uncertainty to achieving your objectives. If risks do not appropriately relate to your objectives, you run the danger of having directionless efforts.

To ensure risk management is objectives-centric, ensure that you put your objectives at the heart of the risks that you identify, analyse and manage – and also for the issues that have occurred that you need to respond to. Think through large-impact possibilities and stress test them; don’t just think about risks that you think will have the largest likelihood – we can’t see the future, and we need to plan for large-impact possibilities.

Make sure that your assurance programme verifies that this is being done effectively.

3. Organisational environment and culture affects the importance that people attach to managing risk

Why is it important?
Peter Drucker is also quoted as saying that “culture eats strategy for breakfast”. His point is that if you get your culture right, good things will happen.

How does it matter?
The culture of taking and managing risk starts with leadership at the top. How leaders address and communicate risk is crucial to how risk management is undertaken. Leaders need to “walk the talk”, by using the forums they take part in across their organisation to discuss the importance of managing risk well, and in a common way. Do leaders always seek to include words and phrases about the importance of managing risk in their addresses and communications?

A defining feature of a good culture for managing risk is that people will openly and collaboratively identify risks, then agree the best actions to manage them, and then monitor them.

What to look out for
The organisational culture for managing risk is underpinned by people’s attitudes and behaviours. Do you know if the attitudes and behaviours towards risk of people in your organisation are aligned with your organisation’s objectives? Are people clear on what is expected of them, and is their understanding of risk consistent with how risk is communicated and discussed at a management and executive level?

People’s attitudes will be influenced by their performance goals and objectives. This is an important aspect to consider when assessing risk culture, particular with regard to rewards and incentives on offer.
To assess your organisational culture towards risk, conduct structured interviews and surveys of a cross-section of people in your organisation. This provides valuable insights for a leadership team to understand the culture that exists, and to determine whether any action is required to optimise the management of risk.

The Institute of Risk Management (IRM) has conducted valuable research into Risk Culture.

Table 1 below provides an example of questions that can be used to assess an organisation’s culture towards risk.

<table>
<thead>
<tr>
<th>Nr</th>
<th>Theme</th>
<th>Issue</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tone at the Top</td>
<td>Risk Leadership</td>
<td>Is there a distinct tone at the top from senior management as to the importance of risk management? If so, what does it feel like?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Is direction provided on how risk management contributes to achieving objectives?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Is senior management commitment visible and sustained over time?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Who is the executive sponsor of risk management?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>What tangible actions are visible from the executive sponsor?</td>
</tr>
<tr>
<td>Nr</td>
<td>Theme</td>
<td>Issue</td>
<td>Details</td>
</tr>
<tr>
<td>----</td>
<td>---------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>Dealing with bad news</td>
<td>Do leaders encourage risk information and &quot;bad news&quot; to be actively and rapidly communicated up the organisation?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Are people raising concerns supported and encouraged?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>How are those who transmit bad news treated once it is communicated?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Accountability &amp; Governance</td>
<td>Accountability and ownership for managing specific risks is clear</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>Accountability and ownership for risk management as a process is clear</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>How are these accountabilities documented and communicated?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>What communication and review structures are in place to ensure risk decisions are effectively reviewed?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>How does the Risk function support the governance of risk within the organisation?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Risk Transparency</td>
<td>Is risk information transparent and communicated appropriately up the organisation?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Is strategic direction provided clearly by senior management on appropriate levels of risk taking?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Is appropriate and successful risk-taking celebrated and role-modelled across the organisation?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does the organisation actively learn from adverse events and situations where risks were not appropriately managed?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Risk Resources</td>
<td>Does the Risk function have access to senior management to deliver its remit?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Competency</td>
<td>Does the Risk function have the credibility across the organisation to deliver its remit?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does the Risk function have the resources required to deliver its remit?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Is the Risk function encouraged to facilitate discussions on key risks?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Is the Risk function supported in challenging decisions related to key risks?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Risk Skills</td>
<td>Is it recognised that risk competence and capability are key assets within the organisation?</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Are internal controls seen to rely on a high degree of risk awareness within the organisation?</td>
<td></td>
</tr>
<tr>
<td>Nr</td>
<td>Theme</td>
<td>Issue</td>
<td>Details</td>
</tr>
<tr>
<td>----</td>
<td>----------------</td>
<td>------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td>Informed Risk</td>
<td>Decision</td>
<td>- Is a specific ‘Concern for Risk / Risk awareness’ defined and tracked through the performance management process?</td>
</tr>
<tr>
<td></td>
<td>Decisions</td>
<td></td>
<td>- How are risk skills encouraged and developed?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Is risk information transparent to decision-makers in a timely manner?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Is it possible to determine what boundaries and risk appetite criteria decisions are being made within?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Is it possible to see how risk has been integrated into decision-making?</td>
</tr>
<tr>
<td>8</td>
<td>Decision-making</td>
<td>Rewarding appropriate risk-taking</td>
<td>- Are appropriate risk-taking behaviours rewarded and encouraged?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Are inappropriate or unbalanced risk behaviours (overly risk averse or overly risk seeking) challenged and sanctioned?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- How are appropriate behaviours valued and nurtured?</td>
</tr>
</tbody>
</table>

Table 2 below describes actions that help to reinforce a good organisation culture of managing risk:

<table>
<thead>
<tr>
<th>Action</th>
<th>Expected outcome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stitch key culture elements into decisions</td>
<td>Key cultural aspects that will be focused on are embraced.</td>
</tr>
<tr>
<td>Stitch key culture elements into governance</td>
<td>Governance has the right “tone for risk”.</td>
</tr>
<tr>
<td>Understand your culture with supply chain</td>
<td>Major suppliers use risk culture to make good decisions and be “open”.</td>
</tr>
<tr>
<td>Reward risk-taking</td>
<td>People use the organisation’s ‘Risk Appetite’ properly.</td>
</tr>
<tr>
<td>Be transparent and ask for help</td>
<td>Be transparent about your real risk profile, and ask for assistance from your parent organisation(s).</td>
</tr>
</tbody>
</table>
The importance of accountability
In order for risk is managed in an integrated manner across an organisation, accountabilities for managing risk across businesses and functions must be clear. When accountability is clear, information and reporting flows from operations through to the businesses and the corporate centre flows through an appropriate governance structure which is focused on business decision-making.

4. Your risk appetite defines what risks to take and how to manage them

Why is it important?
The management of risk using Risk Appetite is a commonly adopted practice in the financial sector. It is less understood and applied in many other sectors and industries. Risk Appetite defines what amount of risk you are prepared to take and how you will respond (and hence how much effort you are prepared to make) to manage risk. It is intrinsically linked to organisational culture and how the organisation is structured.

How does it matter?
Risk Appetite defines your tolerances for risk. It is an effective way to measure performance and to guide what you need to act upon. The principles of risk appetite are described in Figure 7 below:

By defining your propensity to take risk, targets to meet and tolerances within which to operate, risk appetite is an important management tool for people in making decisions about the uncertainties they face.

What to look out for
Some organisations create a Risk Appetite Statement, or a series of Risk Appetite Statements for their businesses, which serve as a written guide or guides on the acceptable levels of risk the organisation is willing to take, and its “upper and lower tolerances” for risk.

A defined risk appetite must link to management objectives, to ensure people know what levels of risk should be taken against their objectives, and the amount of effort and cost required to manage and control risk. The mechanisms for managing risk appetite in financial institutions are quite specific.
For asset-intensive organisations, a simple approach can be a powerful tool to assist with integrated risk management.

If your organisation has not yet defined its risk appetite in one or more Risk Appetite Statements, think about the advantages to be gained by doing so. If your organisation has a Risk Appetite Statement but has not widely communicated it, think about how you should socialise it to capitalise on it.

In order to make risk appetite effective, the appetite for the risks that matter to an asset-intensive organisation (safety, financial, procurement & supply chain, reputational, people-related, legal and so on) should be discussed and reviewed on regular basis by operations management, and applied to the risks faced. Identifying what impact risks have on the organisation’s risk appetite is a simple and effective way of tying risk management and business management together. When this approach is consistently conducted across the operations of an organisation, it provides a portfolio / enterprise view of the “risks to risk appetite” which can generate valuable insights into the biggest threats to your objectives.

Connected data networks in forward-thinking asset-intensive organisations and the digitisation of processes is leading to increased real-time availability of performance data. This can be used to make good real-time risk-informed decisions. If your organisation has a coordinated data strategy, performance against risk appetite can be monitored with the use of such data. Many organisations do not yet have real-time data metrics in place. If this is the case in your organisation, the most practical way to manage risk appetite is to integrate it into how teams evaluate their risks.

**Side-bar 1: embedding risk appetite into the way you work**

*In Industrial business ABC Industries, the organisation’s risk appetite, which has been communicated across the organisation, includes the expectations and tolerances on managing operational cash flow.*

*The controls and actions to manage cash flow volatility are understood by the operating sites. During a Finance team review with the Planning team on a particular site, it emerges that their output schedule is likely to change next month. The team reviews the impact this will have on their cash flow and the organisation’s risk appetite tolerance for volatility. It is calculated to have a large impact, moving towards the upper tolerance limit. It is discussed in a governance review. Additional controls are agreed with Head Office, which, although they have a cost, minimise the cash flow variation. The cost of managing the controls for this risk against the financial benefit they have provided is tracked in a “risk cost-benefits assessment”. The actions are shared with other operations as part of a continuous improvement programme (in case a similar situation is identified early elsewhere).*
5. Anticipate and manage risk: it’s “where the action is”

Why is it important?
Having an integrated organisation structure in place, an environment and culture that promotes open discussion about risk, and clear direction through risk appetite sets a solid foundation for people to then apply good risk management practices as part of their business management practices.

How does it matter?
The management of risk is where people use frameworks and procedures to manage risk through mechanisms such as management reviews, workshops and governance forums. It is the “rubber hitting the road”.

What to look out for
The practical implementation of risk usually starts with a Risk Framework. Your organisation may have one that covers elements shown in Figure 8 below:

An integrated risk framework
How do people anticipate risk in your organisation?

Some key indicators to how well people anticipate risk and uncertainty to the activities they are to perform include:

- Do you fully review scenarios and spend quality time to think through their risks and the effectiveness of controls for those risks?
- Do you get together as a team regularly to review risks, think ahead and form insights that they act upon and measure the cost-benefit of?
- Do you learn with others from the knowledge you all acquire about risks you have faced and how you tackled them, and that which exists in the organisation, and do you ask for help from your Head Office on a regular basis?

Are you using Risk Profiles to link Enterprise and Operational risk together?

Risk profiles are a powerful tool to connect enterprise and operational risk. A risk profile is a risk that has been deemed by your corporate / core team as important to the organisation in order to achieve strategic objectives, and it needs to be shared and acted upon across all or part of the organisation. Tactical risks – even when they are important – are not risk profiles. Your organisation may have perhaps ten or twenty (or more) risk profiles. They should be well-articulated descriptions of enterprise risks, with succinct descriptions of controls that are required to manage them (with particular emphasis on critical controls), and suggested management strategies and actions to take. Risk profiles may be referred to as Principle Risks or Risk Factors. They may feature in an organisation's Annual Report.

Risk profiles add the most value when they are responded to with transparency across the organisation. If your culture does not lend itself to transparency, the use of risk profiles will not be effective – they will more likely be seen as bureaucratic compliance box-checking.
How well do you prioritise your risks?
Most organisations use a risk matrix as a “prioritise and reduce” risk technique. The concept of a risk matrix, which combines impact and likelihood to equate to a risk rating, is one that has been used for decades. The “top right” of a risk matrix typically represents the most important risks to focus on.
Having a risk matrix prioritisation method written into a Risk Framework or procedure does not mean that everyone in your organisation knows that it exists, or that they know how to apply it. Also, you need to make sure that your Board and your Executives sign it off as the right way for the organisation to prioritise risk. You then need to ensure that it is communicated effectively so that people know about it, and that they use it properly in their regular work.

Using a risk matrix to prioritise risks is a starting point. You should look to go further than this.
Discuss the context to risks and consider additional factors to improve your prioritisation of risk.
For example, consider whether the following considerations would be useful:

1. If the risk occurs, would it have a demonstrably large impact to your objective(s)?
2. If the risk occurs, would it have a demonstrably large impact on risk appetite?
3. If the risk occurs, would it have a demonstrably large effect on other risks (either their impact or likelihood)?
4. How effective are current controls to manage this risk? When the control environment is demonstrably effective, the likelihood of the risk occurring should be controllable. If the control environment has gaps, the likelihood of occurrence is higher.

Understanding and evaluating your Control Environment is key
Having the right controls in place to manage risk, and rating control effectiveness and testing your controls, is critical. Controls must be proportionate to the risk: high priority risks warrant a greater focus on controls, and a greater assurance priority. Controls that are “critical” must receive the most attention.
Ensure you have a clear process for the evaluation of controls, and an assurance process that independently tests their effectiveness. A “three lines of defence” model is a good approach to adopt, in which the operations perform its self-evaluation (the first line), functional experts perform their evaluation (the second line) and Independent Audits are performed as independent reviews (the third line).

The Control Environment you operate has a cost. Monitor the cost-benefit of your controls and other actions by how effectively they contribute to managing risk and achieving objectives. If your business performance is unaffected by implementing controls, or worse, if it is deteriorating despite the control environment being perceived as effective, you need to change something.
What “Risk tools” are you using?
People across your organisation should be using a common Risk Toolkit. Part of this Toolkit may be an IT Risk tool, such as a Governance, Risk & Compliance or GRC web-based IT solution to manage risks, controls, events and audits in a collaborative and efficient way.

Other Risk tools that could be part of a Toolkit include the Bow-tie Analysis, Pre-mortems, Critical Controls Management, Contingency Risk, and Quantitative Risk Analysis. Insurance is an important Risk tool, often managed by specific professionals. Interactive “What if? Risk models” and data consolidation to review real-time data flows all help people visualise risk scenarios. The key is that they are used for business management. Some disciplines will use some tools more than others. Appropriate “on the job” training should be planned for and provided.

6. Having good assurance in place is a cornerstone to success

Why is it important?
An appropriate focus on assurance ensures that risks are being managed properly. It is increasingly important in today’s fast-changing business environment that assurance is undertaken. Having “three lines of defence” in assurance is a proven effective management model.

How does it matter?
A robust assurance framework implemented through Integrated Risk Management provides management with insights and findings that contribute to good performance.

What to look out for
Internal Audit has a key role to play in overseeing assurance activities. The Internal Audit team should consider the effectiveness of the Risk Framework when they provide their independent assessment of risk. Independent reviews of Risk Profiles can provide valuable insights.

The Institute of Internal Audit provides good performance standards for organisations to use.

Risk-based assurance is a valuable approach of Internal Audit teams. You need the right organisation structure to be in place, and the Risk and Internal Audit teams working together to ensure it is effective.

An assurance model many organisations adopt today is the Three Lines of Defence, as shown in Figure 9. The third line of defence, Internal Audit, should be independent to senior management, typically answering to the Board. A fourth level is sometimes referred to, of external assurance parties such as external auditors.

This material is owned by Risk Insight Consulting. All rights reserved.
A GRC IT system can help to provide an integrated approach for risk and assurance information and data. It can provide Internal Audit teams with appropriate access to operational and enterprise-level risks, and to determine their own independent risk assessment based on their independent reviews.

The assurance being undertaken across an organisation can also assess how well risks are being managed against risk appetite, and how well the organisation is anticipating, adapting and managing its risk at all levels.

The Environment, Health & Safety (EH&S) team is an important function providing “second line of defence” assurance in asset-intensive industries against Performance Standards and Critical Controls at operations, and working with Internal Audit and the Risk team.

7. Continuously improve to sustain high performance

Why is it important?
Two elements of continuous improvement are important to focus on:

1. Ensuring people learn and continue to improve
2. Measure your performance to ensure that you are adding value

How does it matter?
Capturing knowledge about risks, controls and assurance allows organisations to share knowledge for collective use and continuous improvement. Some knowledge is intangible, and some is tangible.

The organisational structure should be set up to encourage the sharing of knowledge across operations, businesses and functions. The Risk team performs a key knowledge sharing function, as they are a functional team that spans across the organisation. They should be regularly providing knowledge and training to business...
operations and functions through workshops and lessons learned reviews such as look-ahead peer assists and look-back retrospectives.

1. Ensuring people learn and continue to improve
Your knowledge repository, structured in an appropriate way, will provide people with a valuable information source. GRC IT systems can provide a repository. You should define in your organisational procedures how people should hold knowledge capture sessions such as Peer Assists (seeking knowledge before activities commence), After Action Reviews (quick-fire learning during activities) and Retrospectives (structured post-implementation lessons learned). You may also have Communities of Practice or similar networks which help to share knowledge and awareness of good risk management. A Risk team may facilitate and lead one of these networks for risk management.

2. You are what you measure: track your performance to ensure you are adding value
Continuously improve your management of risk by measuring what is working and what is not. It is easy to say that the successful management of risk goes unseen, because “good risk management prevents negative events from impacting your operations”. You should not accept this approach. You should measure the management of risk by weaving measurements into your regular activities. These measurements should be in the form of costs to manage risk, and specific financial benefits achieved by undertaking the actions that are agreed.

What to look out for
The following five points are indications of a good learning culture:
1. When encountering a problem, I reinforce the importance of learning from others - rather than simply providing an answer.
2. I personally demonstrate that “asking for help” is a sign of strength rather than weakness.
3. When reviewing a new initiative, I ensure that we have sought knowledge from other parts of the organisation.
4. I coach my team to network more effectively - internally and externally.
5. My team sees failure as something to learn from, not something to cover up.

The following are two ways to measure the success of risk management:
1. The cost of controls and actions to manage risks, and their effect on project outcomes
2. The cost of managing risk against risk appetite performance and organisation objectives
You are what you measure

1. Measuring the cost and benefit of controls
All controls and actions have a cost. Your finance team sees the bills for them. You can establish an accurate estimate of the cost of controls when the right people are in the room. Ask the question during your reviews. When you track how controls are contributing towards performance, you can demonstrate their financial value (whether they are safety controls, design controls or any others).

2. Measuring performance against risk appetite
By considering your risk appetite in managing risk, you can track performance against risk appetite metrics over time (such as safety metrics, financial metrics, supply chain metrics and others). The idea of tracking performance against risk appetite is to take action before tolerances are exceeded and hence manage risk. You can measure the financial value of actions taken.

Conclusion

Taking the time to plan, implement and monitor the effectiveness of Integrated Risk Management will increase your ability to manage uncertainty, which increases likelihood of achieving your objectives, and your confidence in achieving predictable outcomes. Taking the time to measure your management of risk, and ensuring knowledge is shared to continuously improve, gives you the means to tangibly demonstrate the cost-benefit of your risk management activities.

Figure 10 describes a few pointers of risk management to keep in mind on a daily basis: