airmic

The Changing World of Risk

Guide 2015

Contents

The objective of the guide is to lead risk managers through recent and future changes to the industry, with implementation advice on recent Airmic publications. The guidance outlines best practice to assist risk managers in achieving high standards for current risk management and anticipated future needs. This will be done using the principles of the 2014 Airmic report, Roads to Resilience.

The following documents are referenced in this guide, and can be found on the Airmic website, *www.airmic.com*

Roads to Resilience, Airmic, 2013

2014 Update to the UK Corporate Governance Code, Airmic, 2015

Tomorrow's Risk Leadership, Tomorrow's Company, 2015

Looking through the risk lens – Building reputation and resilience into the business model, CIMA, 2015

1. Introduction

Airmic published its highly acclaimed '*Roads to Resilience*' research in February 2014. In the 12 months since publication, the risk management world has shown its continual propensity to change. During that time, we have welcomed an update to the UK Corporate Governance Code, seen a new Insurance Act signed into law and welcomed the first British Standard on Organisational Resilience (BS65000).

There is no doubt that the challenges of globalisation, digitisation and new technology combined with the pace of change and increasing complexity and aggregation of risks are putting more demands on boards, which retain ultimate responsibility for managing risk and compliance. With the increased transparency of operating environments and the potential need for instant response to any incident, the challenge of becoming and being a resilient organisation is already material and steadily increasing.

What has remained the same is the criticality of good risk management. Organisations continue to face crises. Some of these have been external, caused by unforeseen events or lack of planned response, while others have begun inside the organisation, with senior management taking poor decisions, condoning bad practice or being compromised by the actions of their colleagues. *Roads to Resilience* identified five clear principles that would have allowed these companies to better deal with their situations. Twelve months from publication, the lessons from *Roads to Resilience* remain pertinent and relevant to supporting business success.

This guide has three main aims:

- Changing risk requirements: to provide risk managers with an understanding of the changing governance and risk management expectations of the board and guidance on how to approach the new challenges
- Changing role of risk managers: to support risk managers in understanding the challenges they face in elevating their role from risk manager to risk leader and in moving to an environment with risk leadership expectations
- Changing risk process: to give risk managers recommendations on how best to measure resilience so that they can ensure resilience across all five principles and to provide practical advice on how to improve resilience.

2. The changing world of risk management

The value of risk managers has long been recognised and the level of influence held by the most senior risk managers is increasing. Risk and reward are key drivers for the ongoing success of any organisation, and risk management underpins strategic decision making. Companies take risks to generate returns. As the focus on risk management increases, it is the responsibility of boards and risk managers to ensure that current risk management practices meet anticipated needs.

2.1 Changing requirements: The Board and Financial Reporting Council guidance

Updated Financial Reporting Council (FRC) guidance, '*Risk Management, Internal Control and Related Financial and Business Reporting*', was published in September 2014 and implemented for all companies reporting accounts from 1 October 2014. The guidance replaces the '*Turnbull Report*' (2005) and states that ultimate responsibility for risk management and internal control rests with the board. The guidance also states that risk management should support better decision-making, rather than inhibit sensible risk-taking, in line with growth strategies and operations.

The risk guidance states that economic developments and some high-profile failures of risk management in recent years have reminded boards of the need to ensure that the organisation's approach to risk has been properly considered when setting strategy. The guidance emphasises that the board's responsibility for the organisation's culture is essential to the way in which risk is considered and addressed. The assessment of risks should:

- Be part of the normal business planning process
- Support better decision-taking
- Ensure the board and management respond promptly to risks when they arise
- Ensure shareholders and other stakeholders are well informed about the principal risks and prospects of the organisation.

While risk managers may have day-to-day responsibility for implementation of risk management processes, it is up to the board to ensure that the appropriate systems and policies are in place. The board needs to ensure that understanding of risk is high, that risks are maintained within tolerable levels and that risk mitigation is appropriate. In fulfilling these more onerous risk responsibilities, boards will require the help and support of risk management professionals. There is a clear and developing need for in-house risk management expertise to help boards and management fulfil the obligations laid out in the FRC guidance.

Full guidance on the implications of the FRC guidance and its impact on the risk manager can be found in the Airmic guide, '2014 Update to UK Corporate Governance Code', published in May 2015.

The risk guidance published by the Financial Reporting Council (2014) to replace the Turnbull Guidance (2005) represents a significant development in the risk management and internal control obligations placed on the boards of companies. In fulfilling these more onerous risk responsibilities, boards will require the help and support of risk management professionals. There is a clear and developing need for in-house risk management expertise to help boards and management to fulfil the obligations

Source: 2014 Update to UK Corporate Governance Code, Airmic, 2015

2.2 Changing role: Risk Manager today, Risk Leader tomorrow?

As the requirements of risk managers change, the role of the person fulfilling these duties must also change. In May 2015, Airmic participated in collaborative research, '*Tomorrow's Risk Leadership'*, with Tomorrow's Company which suggested that there is a requirement for all companies to have a senior executive responsible for risk management. In the past, this role has typically been a mandated role, required by the regulators to ensure compliance. The case has now been made for the individual in this role to be a key strategic partner and a trusted advisor to the board, senior management and decision-makers.

If the case for this type of role has been made, risk managers need to ensure that they have the right capabilities, skills and competencies to successfully fulfil them.

The changing brief remains based on sound technical foundations but also emphasises the ability to build relationships and deliver effective challenge with a broad base of business knowledge. A risk leader upholds the principles of risk management – to protect the balance sheet and ensure ongoing viability – but adds to this, with stronger ties to business planning, business models and strategy. Crucially, the risk leader must retain the impartiality and honesty that has always been vital to the role.

As well as acting in a supporting role to the board, ensuring that it meets its duties in relation to risk, the risk leader can also contribute towards the development and execution of strategy and opportunity. By acting as 'Risk Counsel' to the board, the risk leader plays an essential role in the measurement of risk and reward in the process of decision-making.

The success of this position depends on a number of key responsibilities. Ensuring that the business has a deep understanding of the relationship between risk, reward and strategy will embed the risk process across the organisation. Leading the risk culture should mean that the business will proactively deal with risks, engage all employees and minimise the impact at times of crisis.

To achieve this position, risk managers must ensure that they have a broad base of business skills, as well as technical risk skills. A risk leader will require their skills in influencing and negotiation, in people management and in forming strategic partnerships to be just as strong as those in risk identification or mitigation. They must have a view of the entire business and so will be able to add value across all areas of an organisation.

The full paper, '*Tomorrow's Risk Leadership'*, can be downloaded from the Airmic website.

> ...this publication puts forward the case for all organisations to rethink their risk leadership and consider the value of a dedicated executive risk leadership role, taking into account how risk is structured in the organisation and its risk maturity. The role is not about removing the responsibility for risk from members of the board. It is to help support them in managing today's and tomorrow's risk agenda. Having in place an executive voice of risk in the organisation that leads the risk agenda helps deliver the business model and drive business performance.
>
> *Source: Tomorrow's Risk Leadership, Tomorrow's Company, 2015*

While risk management has developed significantly in recent years, a new integrated approach is needed, which provides a complete and coherent picture of the organisation's risk universe. We believe that organisations can achieve this by viewing their business model through the lens of risk – and within the context of the external environment

Source: Looking through the risk lens – Building reputation and resilience into the business model, CIMA, 2015

2.3 Changing process: a resilient risk function

Changes to risk leadership encompass not only the person and the role, but the way in which risk is managed as a whole. A risk leader will ensure that their team is fit for purpose, that processes are robust, information is clear, roles and responsibilities are defined and embedded in role profiles and reward systems, and that all of these are appropriate for their organisation. To do this, risk management will move from what might have been viewed by some to be a reactive, silo and compliance-based process to one that is proactive, dynamic and influential.

Airmic's recent publication with the Chartered Institute for Chartered Accountants (CIMA), '*Looking through the risk lens – Building reputation and resilience into the business model'*, gives advice to members of both organisations on using the business model to ensure that all risks are effectively captured, mitigated and monitored. While strategic risks are the domain of the risk leader, clear and conscious effort must be made to identify, mitigate and monitor all risks. Using the business model to do this will ensure a thorough understanding of the risks of current operations within the context of the internal and external environment, and provide a sound basis for identifying risks and opportunities.

The Risk Transformation

From...	To...
Compliant governance	Proactive stewardship
Operational and tactical risk management only	Strategic risk Management included
Partial, fragmented and static risk controls	Robust, intergrated and dynamic risk controls, aligned to risk appetite
Organisationand system silos	Cohesive organisation and intergrated systems
Risk applied to objectives	Risk applied across the business model
Eliminating downside	Facilitating upside
Risk manager	Risk leader

2.4 The role of Resilience

A resilient business will meet the needs of the changing world of risk management by using a clearly managed process to achieve the requirements of today's organisation and support the risk manager in becoming a risk leader. Resilience is a key indicator of future business success. *Roads to Resilience* **showed that the incentive to become resilient goes well beyond merely avoiding disaster. Organisations that are confident in their risk management translate that confidence into being more enterprising and entrepreneurial, thereby not only identifying risks but also seizing opportunities. Strong performance in an increasingly risky world combined with potential for growth is the ideal position for a business to be in. Resilience ensures that an organisation retains a wide focus with the internal and external environments, the short-term and long-term strategic aims, and the proactive and reactive methodologies considered throughout the principles.**

As well as the practical improvements to risk management achieved by resilience, there are benefits to the risk manager, allowing them to move towards risk leadership. The networks and relationships built by resilience are the foundations to the partnership required by a risk leader. The exceptional risk radar will allow for strategic discussion and build the wide business knowledge that is required to be a true risk leader.

For these reasons, achieving resilience is not a stand-alone objective, but part of a wider change in the role of the risk management and the risk manager in the most successful organisations.

3. Principles of Resilience

In this section, there is a Road Map to Success for each principle, as well as ten tips to achieving resilience in this area. While not exhaustive lists, they reflect the critical areas for each principle.

To achieve resilience, the risk manager must first understand the current levels of resilience within their organisation. These levels may vary across principles and show areas requiring further work. They will also show areas of strength. When discussing risk management with the board or senior management, these indicators will enable open conversations to assist the board with understanding risk profiles, seeing where resource is required and ultimately helping to fulfil the board duty to ensure robust risk management.

In this section, you will find the checklist for scoring each of the five principles for resilience. These questions will give a total possible score of 16 for each principle. In order to consider your own organisation and prioritise any actions, you may find these useful to give an idea of the current levels of resilience. These are not definitive, but sample indicators of high performance. Totals for each section should be viewed as follows.

Score	Result
0–4	This principle is underdeveloped and needs urgent action
5–8	This principle has foundations in place, but with room for increased resilience
9–12	This principle is embedded, with some finessing possible
13–16	This principle demonstrates a high level of resilience

In addition, there is member feedback on each principle. A sample of the Airmic membership was surveyed in January 2015 to provide suggestions on how to implement each principle. As well as this, they were ask to rate each principle according to how resilient they were 12 months ago, are currently and anticipate being in 12 months. They were also asked to rate principles in order of priority for their organisation.

3.1 Principle One: Risk Radar

The principle of the risk radar is to ensure appropriate mitigation of identified risks and to provide an early warning system for emerging risks.

1. **Employees and stakeholders: risk management communicated and embedded**

   Risk management may be well embedded at a senior level, but all employees and stakeholders should be aware of how to raise a risk, report an incident or near miss, or signal early warning signs of an event. This could be through a risk management forum, risk workshops or training.

2. **Appropriate tools for each level used**

   Attitude to risk may vary at different levels of the organisation. Principal risks must be reported to the board, where an operational risk may be managed at an appropriate level. Policy, process and procedure should reflect the correct tools to be used and information required for differing levels of risk.

3. **Vigilance constant**

   All employees must be able to recognise a potential risk or the warning signals of a possible event. If risk management is solely review based, this information may not be considered until it is too late to mitigate or after an event has taken place. An intelligence network is required, both internally and externally for key suppliers.

4. **Complacency avoided**

   Overconfidence in the risk management process can lead to risks being overlooked or underestimated. Due process must be in place and procedures followed to prevent this.

5. **Questioning open and empowered**

   Employees at all levels should be encouraged to ask honest questions of others, including superiors. This communication will give objective and critical feedback, which is vital to constant improvement of risk management.

6. **Identification process including horizon scanning strong**

   Identification of risks is key to a strong risk radar, which considers identified risks, risks with the potential to increase and a scan of emerging risks. While structured reviews will allow for this, employees should not have to wait for those reviews to raise a risk. Looking at future or emerging risks is critical to understanding the full risk profile and preparing for possible events.

7. **Risk, incident, near miss and shadow registers dynamic**

   Registers can become a list of words on paper, as opposed to a tool to understand and appreciate risk. Registers should be living documents, constantly updated to reflect the current situation. A risk register that is static shows that an organisation is not actively managing risk, considering the potential changes to consequences and likelihood, reviewing incidents, or evaluating and learning from near misses.

8. **External indicators considered**

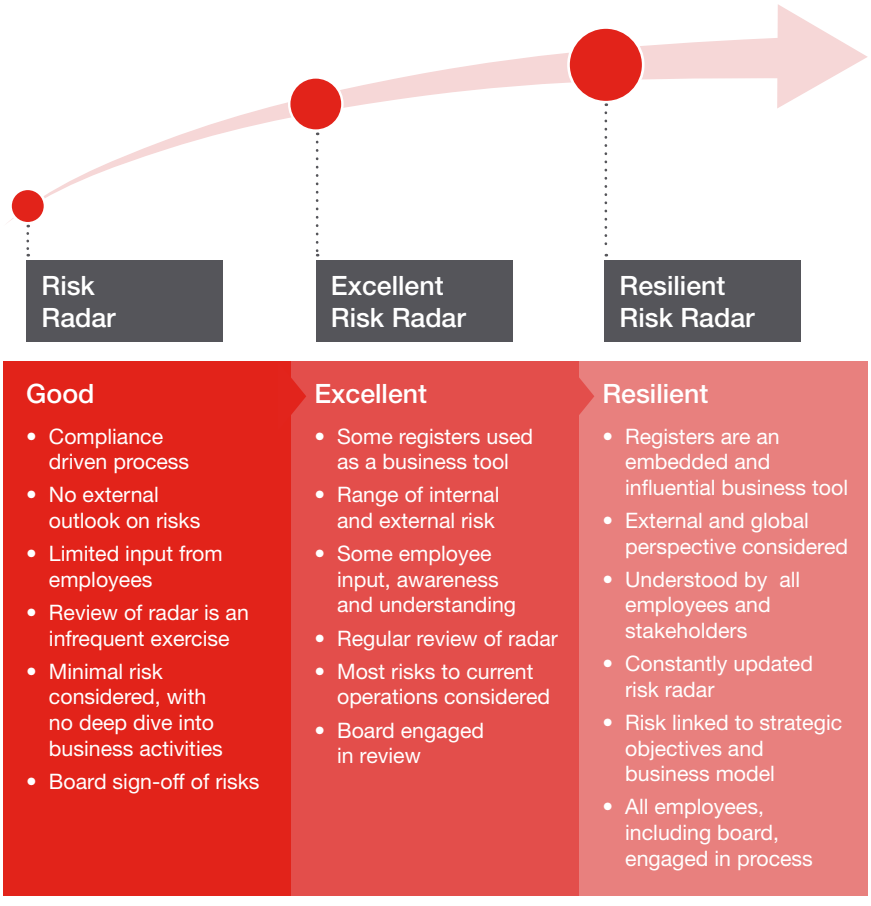
   Risk radars should account for changes outside of the business. A change in legislation, environment or a global financial or health crisis could impact an organisation's ability to succeed. The radar must reflect the external risk factors as well as the internal risk factors.

9. **Culture of sharing with suppliers and contractors established**

   Having a strong internal risk culture will shape the risk radar, but to be truly resilient, key suppliers, contractors and third parties should share in the culture. They should be able to flag any concerns or potential issues, just in the way that employees can. To achieve this, all suppliers must be made aware of the expectation for them to do this, just as with employees.

10. **Cross-functional reviews conducted**

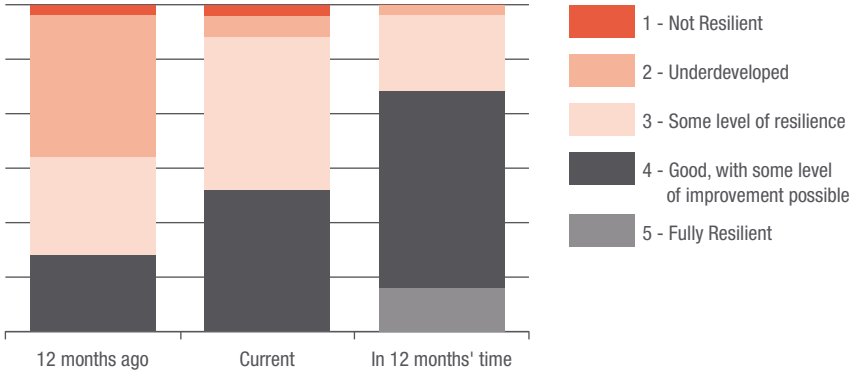
    Managing risks within silos can mean that risk is not appropriately understood and aggregated across an organisation. Similar risks could be managed differently across functions or, when combined, could increase the level of risk faced. For this reason, risks must be consolidated across the business and reviewed by a cross-functional team.



Member Feedback

From the January 2015 survey of a sample of Airmic members, risk radar ranked as the most important principle for 30% of our surveyed members, the second-highest of any principle. It also shows one of the greatest improvements in resilience over the last 12 months, with only 10% now believing this principle remains underdeveloped.

Principle One : Risk Radar



Members with success in this area suggested a number of techniques:

- One-to-one meetings with the board members allowed a more focused discussion on their own challenges and helped to guard against 'groupthink'. These supplemented the whole board sessions, but did not replace them.
- Deliver information in manageable chunks. Boards and senior management can be overloaded with information from various sources – take the time to deliver relevant information in digestible pieces to make sure messages get through.
- Collaborate! By including business continuity and insurance specialists in the conversation, a broader picture is built and the risk and its impacts are better understood.
- A shadow risk register or watch list allows visibility of emerging risks and starts the discussion of these early on. The board becomes aware of risks before they are big enough to reach the risk register, and at a stage when they can be easier to manage.

Enabling Risk Radar

Effective risk radar is achieved by ensuring a high involvement of stakeholders, constant vigilance and avoidance of complacency, as well as creating an environment where everything is challenged and questioned. It is also about ensuring open and effective communication throughout the organisation and its networks to avoid the board risk information 'glass ceiling' and the 'glass walls' between functional areas that results in board risk blindness.

Source: Roads to Resilience, Airmic, 2014Principle One: Risk Radar

High Involvement (Score one for each)	
Do these groups understand their role in risk management and fulfil their risk responsibilities?	
- Senior management team	
- Senior leadership / board	
- All employees	
- Contractors, supply chain and other external partners	

Constant Vigilance (Score one for each)	
When is risk management prevalent?	
- Annual sign-off and reporting	
- Regular scheduled intervals	
- Used in strategy, tactics and projects, including M&A and disposals	
- In horizon scanning and planning activities	

Avoiding Complacency (Score one for each)	
At which of these times is an emerging issue or risk raised?	
- At a scheduled review	
- When a potential issue arises or an event occurs	
- When a near miss happens	
- After an event	

Challenging Questioning	
- Are all employees encouraged to challenge?	
- Are risks sense-checked by a wider audience than the person reporting the risk?	
- Are all employees empowered to challenge?	
- Are reports of near misses and events reviewed to challenge policies and/or procedures?	

Total for Principle One: Risk Radar	

3.2 Principle Two: Resources and Assets

Planned allocation of resources and assets anticipates the need for flexibility and diversity, and makes the best possible use of resources at any time.

1. **Strategy and tactics must be aligned with risk appetite**

   Changes to strategy or tactics may lead to higher levels of acceptable risk, while core functions may be tried and tested, with low levels of risk. This must be considered in the overall risk attitude so that unnecessary risk is not taken but there is enough flexibility to achieve growth and goals.

2. **Single points of failure must be eliminated wherever possible**

   Single points of failure can lead to shutdown of operations or can increase risk, as little oversight is in place. This extends to all areas of operations, including products, employees and partners. As much diversity should be in place as possible to prevent critical failures.

3. **Critical resources and assets must be identified**

   Stress testing and scenario testing can point to critical individuals, tasks or processes that are vital to operations. These should be known and protected through the resource and asset planning process.

4. **Dependencies should be limited**

   As with single points of failure, dependencies on one customer, supplier or even investor can be dangerous as a failure of that key partner could lead to a halt in operations. Dependencies on external parties should be limited as much as possible, particularly as these are largely out of the control of the business.

5. **Change and innovation should be encouraged**

   Many companies fall into the trap of doing things as they have always been done. Change and innovation can improve efficiency, drive down costs and lower risk. They should be welcomed and encouraged.

6. **Awareness of risk and associated resources is embedded**

   An awareness of risk and its association to resources and assets will improve the standard of risk management as key people, processes and products can be highlighted and protected. Mindset and behaviour will shape culture, which allows an organisation to flex as necessary.

7. **Resources and assets are organised for maximum flexibility**

   Changes in the global economic environment could lead to a change in strategy from a business. For this reason, the resources and assets must be flexible to adapt to these changes and protect the income of a business.

8. **Capacity can be increased to adapt to sudden and unforeseen circumstances**

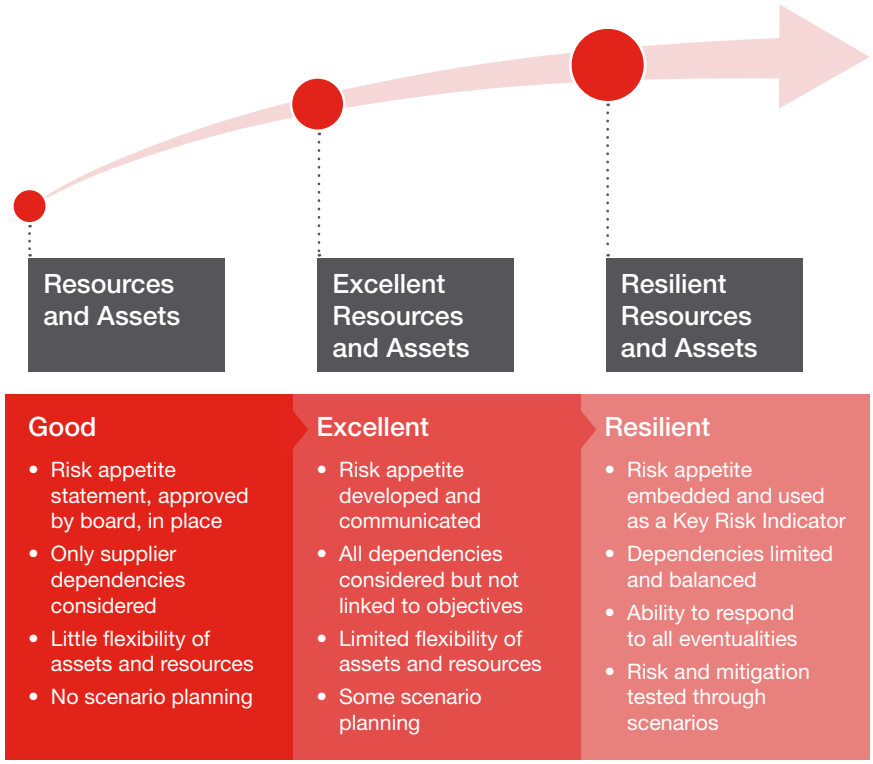
   By understanding the resource and asset requirements of an organisation and matching these with priorities and requirements, a business becomes more resilient in the face of unexpected risk. The increased fluidity allows for greater adaptation, while conserving what is required for key functions.

9. **Plans for contingencies are in place and rehearsed**

   When working on large projects, contingent resources should also be worked into planning. These may be financial, extra available man hours or room with delivery dates so that projects are completed to the highest possible standards.

10. **Risk appetite is defined, understood and embedded**

    All employees should be empowered to take risk decisions within the appetite of the organisation. In order to do this, risk appetite must be set at the top and communicated to all employees.



Enabling Risk Radar

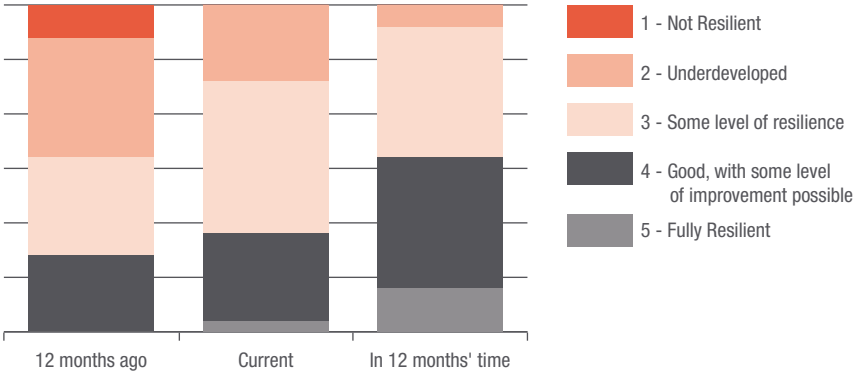
Developing resilient resources and assets requires the organisation to have a clear understanding of its operational risk appetite and the need to limit dependencies. The attitude of the board to risk is also a key issue when resources and assets are deployed to implement strategy. One of the most important components is that the organisation has built flexibility into how resources and assets are selected and deployed. Finally, resilient organisations undertake scenario testing to prepare for the expected and to ensure that they can cope with the unexpected.

Source: Roads to Resilience, Airmic, 2014

Member Feedback

This principle showed a wider spread of prioritisation and appeared rated in every category, from 1 to 5. The majority placed this principle towards the lower end of their priorities. Responses to predict improvements were relatively stable, with most people anticipating being one stage closer to resilience in the coming 12 months.

Principle Two : Resource and Assets



Members with success in this area suggested a number of techniques:

- Empowering employees meant that they understood what good looked like and worked to achieve this. This meant that risk managers did not have to 'police' all activity; instead, their role was more about education and support.
- Ensure the risk function is at the table early when making key decisions. This ensures that upside and downside risk can be considered, and shows the value of good risk management by ensuring that contingencies are in place when necessary.

Risk Appetite (Score one for each)	
Is risk appetite:	
- Defined?	
- Communicated?	
- Considerate of various business activities?	
- Consistently measured across the organisation?	

Limit Dependencies (Score one for each)	
Are dependencies:	
- Balanced between high and low risk?	
- Reduced where possible and desirable?	
- Considerate of more than just supply?	
- Contingent?	

Build Flexibility (Score one for question answered yes)	
- Can resources and assets fluctuate when necessary?	
- Does planning account for all impacts across the organisation?	
- Are potential responses to events considered?	
- Are contingencies built into strategic plans?	

Scenario Planning (Score one for each)	
Are scenarios in place which:	
- Identify potential risks?	
- Identify suitable responses?	
- Challenge the assumptions?	
- Clarify resource implications?	

Total for Principle Two: Resources and Assets	

3.3 Principle Three: Relationships and Networks

Relationships with suppliers, partners, customers and contractors should have a common purpose and allow for rapid and open conversation if an issue arises. This will ensure quick and appropriate responses.

1. **Define the common purpose**

   All people in the organisation, suppliers and contractors should be working to a common purpose to ensure that everyone moves in the same direction, with the same focus and for the same reasons. This purpose needs to be communicated and understood by all.

2. **Engender trust**

   Across the organisation, there should be trust between departments, levels of management, and internal and external stakeholders. By having open and honest conversations, this trust can be built and will support a rapid response when necessary.

3. **Good relationships build reputations**

   The common goal and trust within an organisation becomes visible from the outside, which strengthens reputation. As reputation and brand are vital to ongoing success, having good relationships becomes critical.

4. **Ensure perspectives and knowledge are shared**

   All people in the organisation should be able to raise questions, openly discuss risks and potential mitigations, and share information. This network increases situational awareness, making a business more resilient through knowledge.

5. **Create a no-blame culture**

   Mistakes must be treated as such if an organisation expects these to be raised quickly and ensure potential bad news or information about issues where improvements could be made is not withheld. Whilst accountability for making mistakes must remain, fear of recrimination may lead to non-reporting of incidents or near misses.

6. **Learn from mistakes**

   Circumstances leading to mistakes and the results of them must be reviewed to look at the cause and the outcomes. Learning from these is important for constant improvement in the level of resilience.

7. **Ask for advice**

   A characteristic of an open and supportive culture is to allow questions to be asked, no matter how big or small. All people should feel able to speak openly as part of a bigger team working to a common goal. As part of a no-blame culture, open questions, no matter how challenging, should be encouraged.

8. **Consider whether your structure works**

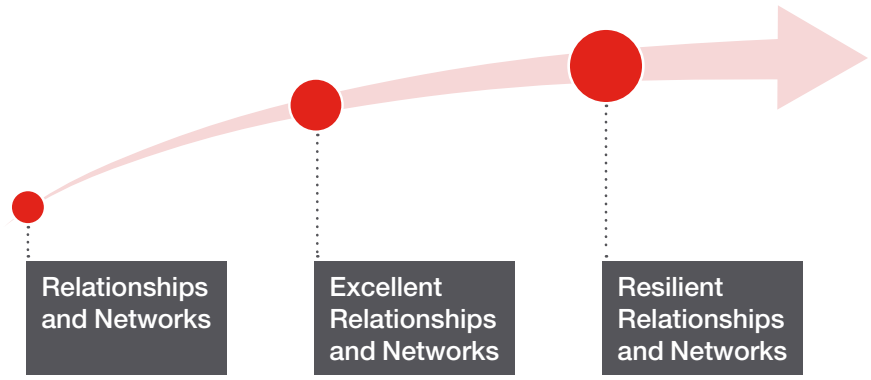
   Hierarchy can create difficulties in open communication. With more layers to travel through, information or messages travelling upwards or downwards can be misinterpreted. The structure of the business has to support communication, including risk communication, for which a flatter and more integrated structure can work most efficiently and effectively.

9. **Align personal goals and strategic goals**

   Everyone needs to have a clear understanding of their own role, and its impact, relationships and contribution to the overall goals of the organisation. For this reason, demonstrating a link between personal objectives and the operational and strategic objectives of the organisation can be useful in signifying the importance of each role in achieving the common purpose.

10. **Leading by example**

    The board or its equivalent is responsible for setting the vision, values, culture and risk appetite of the organisation. Risk appetite should be articulated and leaders should embody the culture of the organisation and be visible in so doing. This will help to promote the importance of risk management.

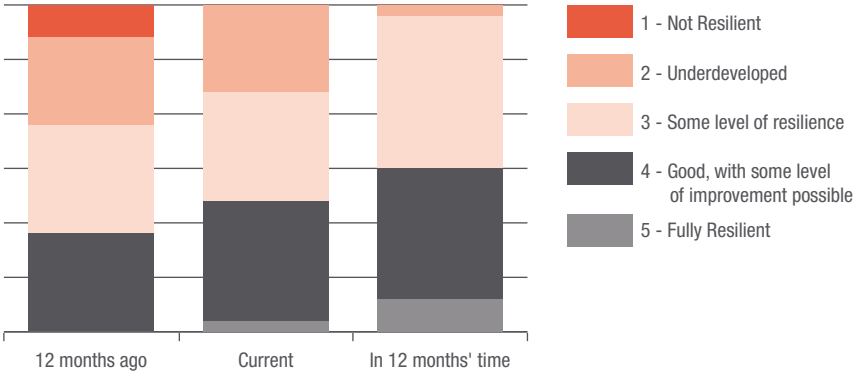


Good	Excellent	Resilient
• Departmental values and relationships defined • Not all events and near misses reported • Basic communication strategies • Customers are not referenced in strategy • Corporate values not evidenced in behaviours	• Common purpose and some level of trust across departments • Knowledge sharing • Communication across departments and functions • Customers considered in business model and strategy • Values portrayed by senior management	• Strong culture of trust and shared values across organisation • All incidents and events are shared • Open communication, with no consequences for raising concerns • Strong focus on customers in business model and strategy • Values evidenced by all

Member Feedback

Respondents showed a high level of confidence in their ability to achieve greater resilience in this principle, with few believing it currently was or would remain underdeveloped. This principle sat firmly in the middle of the prioritisation, with three-quarters of risk managers placing this principle as their second, third or fourth priority.

Principle Three : Relationships and Networks



Members with success in this area suggested a number of techniques:

- Form partnerships with key stakeholders within your organisation, as you would with insurers. They are equally key to good risk management.
- Consider your culture and ensure that it matches your aims. When the culture is supportive of risk management, the job becomes easier.
- A code of conduct could be issued to all members of staff. Communicate the code so that all employees are engaged and can see these values and behaviours are evident from the top of the organisation and throughout, which will help achieve employee buy-in.
- Make risk management a personal objective of every member of staff. By understanding their individual responsibility and being measured against their performance, employees will buy in to the risk culture.

Enabling Relationships and Networks

Resilient relationships and networks are based on shared purpose and values, as well as the existence of a no-blame culture. The presence of good communication within a flat organisational structure will help avoid the risk information 'glass ceiling' and 'glass walls'. Leadership that is fully engaged with the achievement of increased resilience is necessary to deliver a customer focused experience.

Source: Roads to Resilience, Airmic, 2014

Shared Purpose and Values (Score one for each)	
Does the organisation:	
- Have clearly defined values?	
- Have strong departmental and interdepartmental relationships?	
- Communicate a culture of trust?	
- Share the purpose and values with external stakeholders?	

No-blame culture (Score one for each)	
Does the culture:	
- Encourage that no bad news should be withheld?	
- Support whistleblowing where appropriate?	
- Ensure no adverse consequences for individuals raising concerns?	
- Ensure that accountability is maintained?	

Open Communication (Score one for each)	
Does the approach to communication allow for:	
- Effective and efficient risk communications?	
- Cross-functional and cross-team communications?	
- Real-time messages?	
- Bottom-up communication as well as top-down communication?	

Customer Focus (Score one for each question answered yes)	
- Does the customer form part of the organisation's business model?	
- Is customer communication part of rapid response plans?	
- Are customer views and complaints collected, reviewed and responded to?	
- Is customer retention / loyalty measured and responded to?	

Total for Principle Three: Relationships and Networks	

3.4 Principle Four: Rapid Response

This principle will build the capability, resources and relationships to respond rapidly and appropriately to any situation. The Business Continuity Institute Good Practice Guidelines define a crisis as a situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organisation and requires urgent action. Increasingly, crisis management plans are also being termed as rapid response plans. This principle should be embedded in, rather than adjacent to, the organisation's Business Continuity framework and associated plans and processes.

1. **Control a crisis, rather than allow a crisis to take control**

   Crisis management means having plans in place for when things go wrong. Crisis management plans must be designed to take control of a crisis, so that the crisis is carefully managed. As all crises are different, an organisation will need to adapt its plans accordingly.

2. **Link risk response to the risk radar**

   Principal risks should be on the risk radar. As part of mitigating these, plans should be in place for each risk, where appropriate. The risk radar and response plans should be linked, with each informing the other.

3. **Protect your reputation**

   One of the biggest mistakes organisations make in crisis management is using the wrong method of communication, in the wrong way, from the wrong people. An ineffective initial response to a crisis can negatively impact reputation. An early stage of response should consider how best to protect reputation by communicating effectively with stakeholders in an appropriate level. In the digital age, communication is rapid and can come from many sources – crisis management plans must consider this, and ensure proactivity and honesty in communications at all times.

4. **Share responsibilities to consider business as usual**

   Organisations should construct teams to manage crises and business as usual. Having the same team responsible for a crisis as well as day-to-day operations could overburden them. The most effective leaders for a crisis may not be the same as the most effective leaders for business as usual. However, the approach taken to crisis management planning and construction of teams should reflect the business, scale, complexity and culture of an organisation.

5. **Empower employees**

   Employees must be empowered to make decisions and act in times of crisis, particularly if their actions could lessen the impact of the crisis. However, there must be effective communication about how employees should respond and what is expected of them, with training provided as appropriate.

6. **Look for early warning signals**

   A process for identifying signals that give an indication of an impending crisis should be established. A response to these signals should be identified and crisis management plans should include a link to this process and a method of response, including to customers where relevant and where there is a contractual commitment.

7. **Have clear process in place**

   Roles and responsibilities in a crisis should be clear. All stakeholders, including employees, must be aware of the plans for responding to a crisis, how the media will be managed and what their individual responsibility will be. Uncontrolled comments to the media – including those made via social media – must be prevented.

8. **Have well-rehearsed plans**

   Plans must be rehearsed against different scenarios to ensure that they will effectively respond to a crisis. Untested plans could break down during an event, leading to a negative experience for the organisation and failure to achieve operational and strategic objectives. Testing introduces response teams to each other and their responsibilities, as well as giving them an indication of how it would feel to operate in the event of a crisis.

9. **Learn from the results of plan rehearsals**

   When rehearsals are complete, lessons learned must be understood and included in plans. As tests are designed to show inefficiencies or potential improvements, ensuring that these are taken away and incorporated into plans is important.

10. **Choose the right team**

    Crisis management teams will be placed in volatile and unpredictable situations, and may be asked to perform difficult tasks, so ensuring the correct make-up of each team is essential. Teams should be multi-disciplinary and self-organising, with clear lines of reporting and authority. The members must have a breadth and depth of relevant experience, and the knowledge, motivation, empowerment and confidence to make sound decisions in unexpected circumstances.

Good	Excellent	Resilient
• Core team identified • Response plans in place • Plans rehearsed	• Cross-functional response team • Employee awareness of responsibilities • Plans rehearsed and results reviewed • Lessons learned from scenario testing • Plans linked to risk radar	• Cross-functional response teams • Well rehearsed and updated plans • Early indicators identified • Employees empowered to take prevention actions • Business as usual protected in all plans

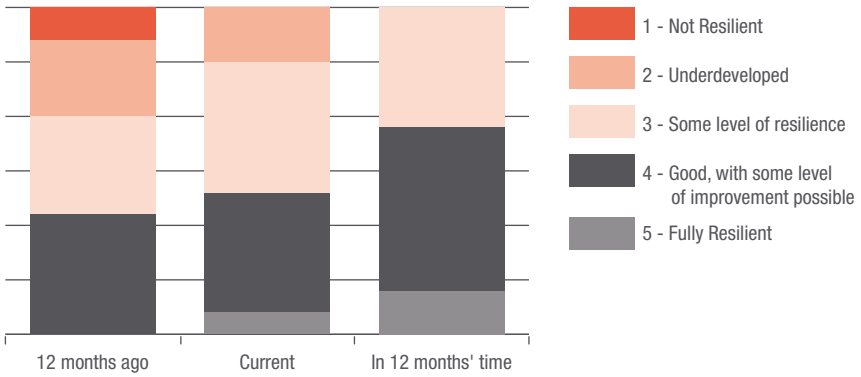
Member Feedback

This principle was not only rated as being the highest priority principle of our respondents, but also the one with the highest levels of success. More participants rated themselves as currently fully resilient in response to this question than any other.

Members who are successful in this principle suggested:

- Ensuring a control centre is in place, whether physical or virtual, so that response is co-ordinated
- Working with Business Continuity Management improved risk profiling, as a greater understanding of the crisis was achieved
- Training and rehearsal of plans helped the business better understand the consequences of a disaster. This leads to understanding the potential impacts.

Principle Four : Rapid Response



Enabling Rapid Response

Achieving rapid and decisive response to changing, challenging and/or adverse circumstances is a key feature of resilient organisations. Organisations need to ensure that identified teams and processes are in place. Rehearsal of potential scenarios is required together with empowered teams to take charge when adverse circumstances arise.

Source: Roads to Resilience, Airmic, 2014

Decisive and Appropriate Actions (Score one for each)	
Do your rapid response plans:	
- Have a link to indicators of emerging crises?	
- Consider risk in the aggregate and the potential for domino effects?	
- Include actions for early intervention to manage escalation of issues?	
- Escalate response when necessary?	

Identified Teams and Processes (Score one for each)	
Do your rapid response plans link to the business continuity framework and:	
- Include cross-functional and cross-level teams?	
- Allow for the concurrent management of business as usual?	
- Empower appropriate decision-making?	
- Tailor existing processes to the given situation?	

Empowered Response (Score one for each)	
Do response plans:	
- Allow flexibility?	
- Consider business as usual?	
- Empower early intervention actions to mitigate consequences?	
- Allow response teams the necessary decision-making powers?	

Well-Rehearsed Plans (Score one for each)	
- Do plans have the flexibility to be used for different scenarios?	
- Have plans been tested against different scenarios?	
- Do plans include defined responsibilities and procedures?	
- Do plans include external experts and suppliers for specific scenarios?	

Total for Principle Four: Rapid Response	

3.5 Principle Five: Review and Adapt

A resilient business is willing to learn from adverse events, near misses and difficult circumstances, and to adapt process, policy or structure.

1. **Structured learning should be in place for all people in the organisation**

   All people in the organisation have a responsibility for risk management and so should receive appropriate training around this. Training should take place at induction, when roles and responsibilities change, and when the organisation changes relevant policies and processes. Training should in any event be refreshed from time to time.

2. **Continual enhancement of processes**

   Risk management processes should be subject to continuous improvement to reflect the current needs of the organisation, anticipated changes, and the constantly evolving internal and external risk environment.

3. **All near-miss events reviewed for learning and improvement**

   Near-miss events should be recorded and lessons should be learned from how the event happened, the drivers of the event and how it was managed. This learning should be used to improve policies and processes, and to update the risk register.

4. **Learning communicated**

   Learnings from events and near-miss events should be communicated to all relevant people in the organisation. Where policies and processes are changed, responsibilities may change, and these changes should be communicated, with training provided as applicable. Examples of good practice should also be communicated as this serves to reinforce responsibilities and practice.

5. **Independent reviews completed**

   As a responsibility of the board, risk management should be independently reviewed. This might involve a non-executive director, a third party or a suitably qualified member of senior management. This will help to ensure that risk management remains robust and appropriate.

6. **Review of board skills completed**

   The board must be able to demonstrate that it has the appropriate knowledge and skills to undertake its responsibilities for risk management and that it has devoted sufficient time to ensuring that the organisation's risk management framework remains appropriate, that risk responsibilities are clearly defined and embedded, that risk appetite is appropriate and communicated, and that it understands the principal risks to the organisation and plans for mitigation.

7. **Post-event structure changes**

   Following an event, the board and senior management must have the ability and willingness to make changes to improve risk management. This relates to Principle Two: Resources and Assets, which requires an organisation to be flexible and adaptable in order to be resilient.

8. **Post-event process changes**

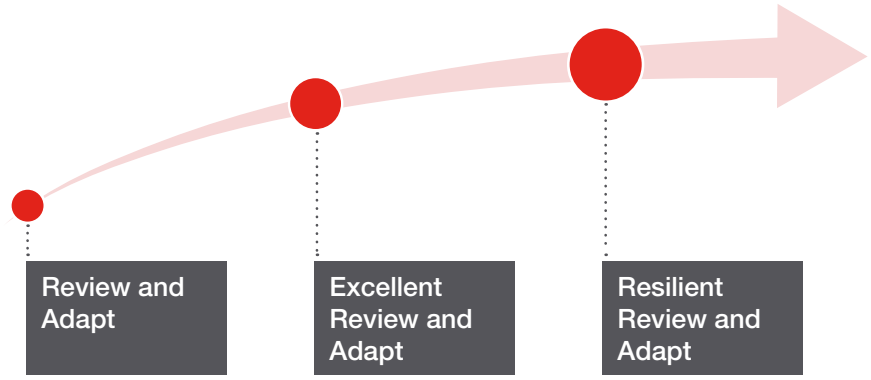
   Following an event, lessons learned from events and near misses will in some cases lead to process change. The risk manager must be sufficiently empowered to work with the board and senior management to ensure these changes take place.

9. **Consider the horizon**

   The environment for all organisations is changing. The risk manager should be aware of changes in the external environment to ensure that they will be able to lead adaptation of the risk management of the organisation to these changes.

10. **Embrace all risks**

    Adapting risk and resilience management to take account of assets which are becoming increasingly intangible is critical. The organisation must consider all risks and the impact these might have on the organisation's delivery of its strategic objectives, and the preservation and enhancement of its reputation.

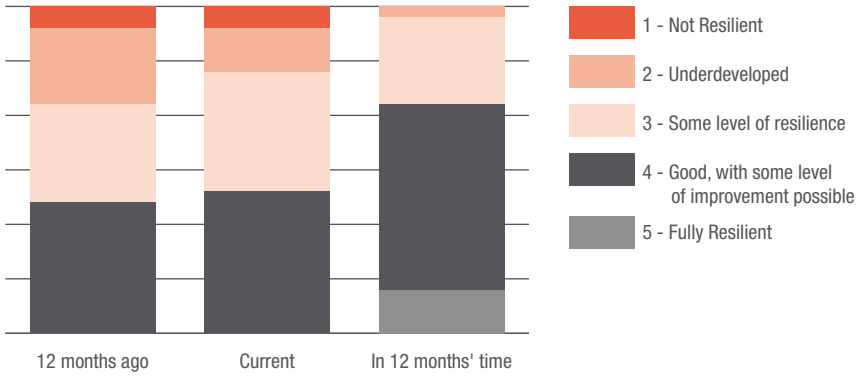


Good	Excellent	Resilient
• Some employee training • Policy updates on a ad-hoc basis • Near miss events reported on a case-by-case basis • Continued enhancement of process and policy completed but findings not communicated	• Employee training for most staff • Continued enhancement of process and policy • Review of some incidents • Communication of some learning	• Structured learning for all employees • Continuous update of process and policy to reflect learning • Every near miss incident reported and reviewed • Independent review completed of process and policy • Communication of all learning

Member Feedback

Largely rated as the less important of the principles, this is one of only two where no respondents rated themselves as fully resilient. Perhaps because of the low importance level for most, the change between 12 months ago and current performance for those rating at some resilience and above is negligible. Looking to the future, there is improvement predicted, showing that while respondents have not placed immediate focus on this principle, they fully grasp that it is equally as important as the others and they intend to make improvements.

Principle Five : Review and Adapt



Members who have been successful in implementing resilience suggested:

- Adding to policies the requirement to communicate near misses has been vital and has made the importance of communication more easily understood.
- Carefully record errors and outcomes as this data can be useful in identifying mitigations
- Understand how the assets the company is protecting are themselves evolving. The economy has evolved over the years and therefore so to have businesses and their assets. The assets behind the share price are today far more likely to be intangible than physical.
- Listen carefully to understand how the context is changing. What was acceptable or true yesterday may not be tomorrow. If you are doing business the way you did it three years ago, you are almost certainly doing it wrong. Risk managers and their businesses must not only adapt to lessons learned but must also anticipate and embrace change.

Enabling Review and Adapt

Organisations need to review adverse events and near misses that occur, learn from the experience and adapt the organisational processes and structure accordingly. A culture of structured learning is required based on independent review of what has occurred or is emerging and a strong desire to constantly improve organisational performance. This same approach is applied to the lessons that can be learned from pursuing business opportunities.

Source: Roads to Resilience, Airmic, 2014

Structured Learning (Score one for each question answered yes)	
- Are processes continually enhanced?	
- Is training relevant and regular?	
- Do all people in the organisation receive risk management training?	
- Is the success of training measured?	

Near-Miss Reporting (Score one for each)	
- Are all events reported and reviewed?	
- Are signals / indicators identified?	
- Are event and post-event findings analysed and communicated?	
- Is loss potential considered for inclusion on the risk radar and/or response plans?	

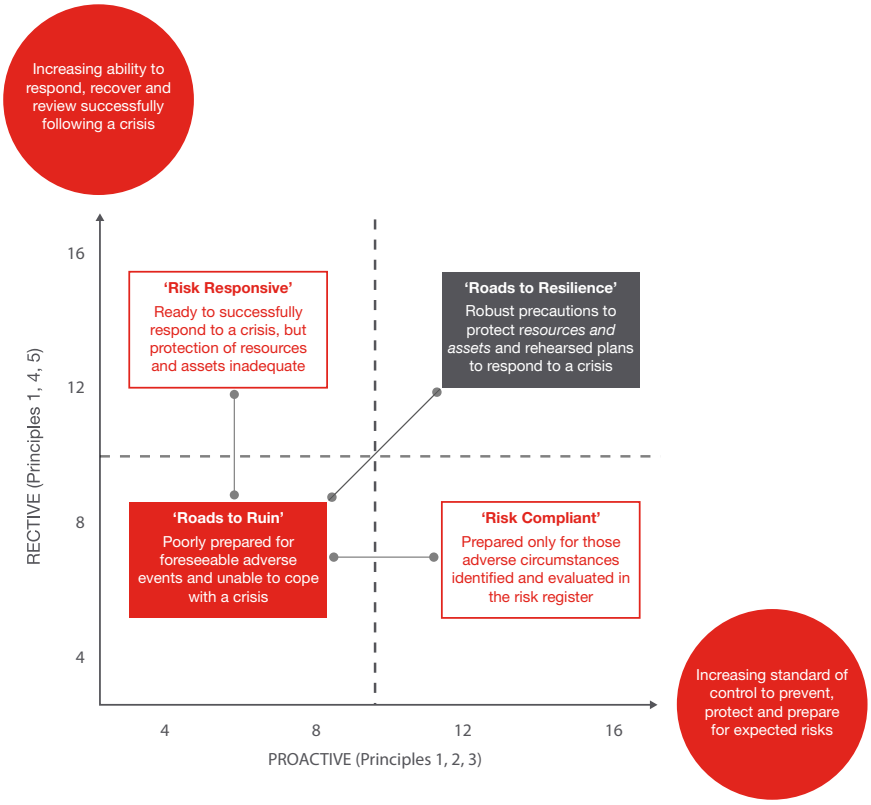
Independent Reviewing (Score one for each)	
Are the following reviewed:	
- Risk management framework and processes?	
- Board activity and skill levels, including NEDs where applicable?	
- Scenario planning and testing?	
- Risk culture?	

Desire to Improve (Score one for each question answered yes)	
- Are changes made where necessary to organisational structures?	
- Are changes made where necessary to organisational procedures?	
- Are lessons learned and reported from events and used to make improvements?	
- Are lessons learned and reported from near-miss events and used to make improvements?	

Total for Principle Five: Review and Adapt	

The scores for each principle should provide an indication of areas of strength or weakness. If scores raise any particular concerns, the risk manager could consider moving through each principle of this guide in order of the lowest scoring section to the highest scoring.

To determine overall resilience, the combined scores of the proactive principles of resilience (principles 1, 2 and 3) can be measured against the reactive principles (principles 1, 4 and 5). This can be mapped against the matrix below.



5. Conclusions

The world of risk management is changing. The risk landscape is constantly evolving and becoming more complex. Achieving resilience in a fast-moving, interconnected and integrated world is a priority for all organisations in order to be flexible, customer focused and alert to threats. Boards are facing increasing complexity, often beyond the immediate experience of individual board members. At the same time, their accountability for effective risk governance has never been more explicit and business practices must be more transparent.

This creates an opportunity for risk managers to provide a critical support function for boards, thereby elevating the role of risk management in the organisation. In doing so, many of the common causes of crises and the fall-out from these would be mitigated. In the 12 months since '*Roads to Resilience'* was published, the sample research indicates that businesses are moving towards higher levels of resilience. By continuing to do this, businesses are ensuring that their ongoing success is protected.

These changes, when taken as a whole, present an opportunity for our profession to continue to promote its value to boards and senior management with whom we will develop a complementary role. Risk managers will become executive partners, or Risk Counsel, to the board, leaders in risk culture, and a vital part of strategy and decision-making. In order to achieve this, today's risk manager must be looking at the changes coming, for their business and their career, thereby ensuring they will remain fit for purpose in the future.

airmic

6 Lloyds Avenue
London
EC3N 3AX
Ph. +44 207 680 3088
Fax. +44 20 7702 3752
email: enquiries@airmic.com
www.airmic.com