ORIC INTERNATIONAL

Creating value from risk events

Leading practices in operational risk event reporting, analysis and investigation, learning and management

Leading practice study by Oliver Wyman on behalf of ORIC

OLIVER WYMAN

FOREWORD

ORIC is a consortium of organisations in the insurance sector with the common purpose of further advancing the management and measurement of operational risk.

One of our key aims is to share best practice in operational risk and, where appropriate, set leading practice for operational risk. We see our mission as serving our membership and creating a community where information and ideas can be shared.

In gathering and sharing information on risk events we also seek to provide practical tools and insights to drive improvement in risk management practices. It is therefore with great pleasure that I recommend this study to you on behalf of ORIC.

We hope this report will inspire you to further improve your own organisation's risk event capture, reporting and analysis. If you operate in the insurance related sectors and you share these values, why not join us on this journey?

Alex Hindson, Chairman, ORIC

IRM ENDORSEMENT

"The Institute of Risk Management is delighted to lend its endorsement to this worthwhile report on the importance of risk event reporting in creating a healthy risk management culture. Our own recent publication on Risk Culture identified the importance of risk disclosure and the effective reporting and escalation of risk events as fundamental tests of an organisation's ability to create a supportive culture. As the world's leading enterprise-wide risk management education institute we see this report as an important step in strengthening leading practice in the area of learning from risk events. Risk events should be seen as gifts to management and as an opportunity to improve. Survival of the organisation may in some cases depend on this important evolutionary skill."

Carolyn Williams, Head of Thought Leadership, Institute of Risk Management

IOR ENDORSEMENT

"The Institute of Operational Risk is pleased to endorse this helpful contribution to the issue of loss event reporting and causal analysis, which is critical to understanding operational risk exposure as well as being fundamental to instilling a learning culture and an environment of continuous improvement. We commend it as a practical guide to those involved in operational risk at all levels."

Simon Ashby, Chairman, Institute of Operational Risk

CONTENTS

EXECUTIVE SUMMARY

Introduction

Operational risk events have resulted in huge losses and reputational damage across all industry sectors. For example, BP faces losses of $43bn as a result of the Macondo disaster; the banking industry has had to pay out tens of billions of pounds in fines and compensation as a result of LIBOR, money laundering, mis-selling and other risk events; and public sector organisations like the NHS have suffered massive reputational damage around patient safety operational risks.

The insurance sector also endures large losses each year from operational risk events, often associated with significant reputational damage. In addition to impacting the P&L directly, capital reserves must be set aside to cover these risk events, which can have a significant impact on corporate return on capital.

Organisations which place a strong focus on risk event reporting, analysis and learning actively reduce operational risk losses. Typically, they exhibit the following characteristics:

- An open culture where people see risk events as an opportunity to improve
- Undertaking analysis of risk events to understand the root causes and establish whether other areas of the organisation could have an exposure
- A disciplined approach to deciding on management actions required in response to a risk event and their implementation
- Continuous improvement of their control framework using learnings from internal and external risk events to reduce operational risk exposures.

When an organisation gets these things right, it tends to outperform the market financially.

Our study

28 ORIC members were interviewed to identify leading practice in risk event management, focusing on risk event capture reporting, analysis and learning. In addition, four companies from other sectors (oil and gas, utilities, aviation, and mining) were interviewed as comparators. From this, best practice approaches were identified and a maturity diagnostic developed to assist organisations in benchmarking and improving their performance. These approaches and the maturity diagnostic have broader applicability across other industries and sectors.

This document is not intended to prescribe particular methodologies. Each individual organisation will be faced with different scenarios, challenges and risks and those working within it will need to use their own judgement to identify appropriate practices.

Main findings

Our study focuses on the four main areas which organisations need to get right:

- Creating an open culture that encourages reporting
- Event investigation and analysis, including impact assessment
- Managing actions
- Learning and continuous improvement.

Creating an open culture that encourages reporting

Creating an open culture where people can speak openly about risk events is fundamental. An organisation that is aware of a loss event or near miss can find ways to create value by reducing the likelihood of reoccurrence and the event's impact.

Identified best practice for creating an open culture includes:

- Making the reporting process as simple and user-friendly as possible
- Ensuring people know what a risk event is, how and when to report it, and how to learn from it
- People feel valued and respected when reporting a risk event and understand the importance of this to their organisation.
- People share information on risk events openly, without fear of blame
- Communication of risk events is timely and efficient, particularly in high priority cases.

Leading practice organisations understand the significance of culture and the role of strong and supportive leadership, risk awareness, understanding and governance in promoting the reporting of risk events.

The crucial ingredient of success is visible leadership behaviour. Best practice organisations have strong, risk-aware leaders who actively champion the process, get involved in training their people, communicate the importance of risk to the business, actively follow up on actions, and recognise people for reporting. Such organisations invest in developing risk leadership skills and measuring leaders' performance in this area. Critically, these leaders avoid blaming those who report, or those who have made genuine mistakes, and place a high value on the opportunity to learn from risk events to drive value for their organisation.

Event investigation, analysis and impact assessment

Effective risk event analysis ensures the business fully understands the root cause(s) of that event to determine the most appropriate response. For major events, this will involve a formal investigation.

Identified best practice for risk event analysis includes:

- Setting clear thresholds that determine when an in-depth investigation of the root cause of a risk event is required
- Using recognised tools and techniques such as: 'The Five Whys'; Fishbone/Ishikawa diagram; and Bowtie analysis to analyse the root cause(s) of material risk events
- Using people with appropriate skills from the first and second (and, at times, third) line of defence to support root cause analysis
- Conducting balanced investigations that cover people, capabilities, culture and behaviours, processes and systems. It is easy to blame a system or human error for a risk event occurring, but it is critical to understand why someone made such a decision
- Evaluating the organisations response to a risk event to identify whether any lessons could be learned.

Accuracy in quantifying the direct and indirect impact of a risk event is important. The true cost (or potential cost), as well as non-financial impacts of a risk event, needs to be fully understood to ensure that mitigating actions are proportionate and to make an effective case for any required changes to the underlying control environment and/or insurances held.

Identified best practice in impact quantification includes:

- Providing staff with a guide that sets out direct and indirect impact types to enable more accurate quantification
- Back-testing of actual losses against the P&L.

Managing actions

The analysis of the causes of a risk event will lead to identification of a number of potential remedial actions. Action management covers the governance and implementation of agreed activities to recover from the risk event itself and to reduce the likelihood of re-occurrence. It is used to find the appropriate balance between potentially conflicting objectives and ensuring all significant actions are carried out, while avoiding the imposition of unnecessary bureaucracy.

Identified best practice in managing actions includes:

- Prioritising actions against a defined risk appetite
- Evidence-based monitoring of the progress of agreed actions
- Meaningful and clear key performance indicators
- Robust governance, including independent oversight
- Assessing the adequacy and effectiveness of actions taken.

Learning and continuous improvement

Organisations need to share relevant key information and learnings from risk events with the parts of the business that could have an exposure. Best practice is also to learn from external events, with a good example provided by the North Sea, where all oil and gas companies openly share details of all safety and environmental risk events, including near misses.

Within the insurance industry, qualitative narratives captured in the ORIC database could be more widely disseminated within members to appropriate first line staff. Through continuous improvement, group-wide operational risk exposures can be systematically reduced. Learning also helps create a culture of ‘chronic unease’. This is an organisational state where people are highly risk aware and continually assessing what might go wrong, as well as being prepared to challenge processes and leaders from an informed basis.

Identified best practice in learning and continuous improvement includes:

- Setting clear targets to reduce annual operational risk exposure
- Identifying relevant external risk events and using the qualitative and quantitative information to challenge the adequacy and effectiveness of internal controls and insurances held
- Sharing information and learnings from internal and external risk events with parts of the business that could have an exposure
- Prioritising and targeting learnings through appropriate engagement. The whole process of learning is most powerful when it is fully integrated into a robust organisation-wide continuous improvement culture.

Conclusions

Currently, there is a wide range of operational risk management practice across the insurance sector. Even organisations of similar scale and in the same area of business show markedly different levels of maturity around their approach to operational risk event reporting, analysis and learning.

Maturity Diagnostic

There is a real opportunity to reduce the cost of operational risk across the industry. To assist organisations in benchmarking and enhancing their own performance we have developed a maturity model. This identifies four levels of maturity:

- **Reactive:** organisations where operational risk events are seen as a cost of doing business, with little focus on effective risk management
- **Compliant:** organisations which focus on meeting rules and regulatory requirements

- **Proactive:** organisations where everyone owns risk and takes responsibility for improving its management
- **High reliability:** organisations where risk management is transparent and fully integrated into continuous improvement systems. Staff at all levels take full ownership of risk and feel free to challenge. The company learns from its own and external loss events and actively targets reductions in operational risk losses.

Moving from 'reactive'

We have identified three key levers for organisations which wish to improve from a reactive approach:

- **Build a compelling benefits case:** covering both financial and non-financial benefits
- **Gain leadership support:** create strong, visible, executive level sponsorship
- **Increase awareness and knowledge:** of operational risks, reporting processes, and the benefits of reporting, through a major engagement programme.

As leaders and staff focus on understanding the operational risks they face and the benefits of risk event reporting, organisations will quickly strengthen their operational risk management. Typically, organisations can expect to see a temporary increase in loss events as reporting improves.

Organisations should be wary of creating a systems and process based solution, although this may meet regulatory requirements. Without effective leadership and staff engagement, such systems-led transformations are notorious for not producing real benefits and for being unsustainable. Successful organisations have initially built simple tools and templates (such as electronic forms) rather than depending on off-the-shelf systems. Improvements to these basic tools can be made quickly and adapted to business requirements. In all but the smallest organisations, this information will then be captured on the corporate risk system.

Moving towards 'proactive' and 'high reliability'

Best practice in other sectors identifies four key areas:

- **Near miss reporting**

  A focus on reducing the incidence of near misses will reduce the number of loss events. Other sectors have demonstrated that addressing near misses will quickly deliver tangible results. Some insurance organisations reported that they treat small loss events as large near misses, but others report difficulties in achieving accurate near miss reporting.

- **Behaviours and culture**

  Best practice in other industries is to give the same weight to addressing behavioural failures as is given to system, control and process failures. Only by focusing on behaviours can organisations become mature. There was almost universal recognition from the insurance companies interviewed that behavioural issues lie at the heart of most loss events. Many report a developing focus on addressing culture.

- **Root cause analysis tools for analysis and investigations**

  Other industries use proven industry-wide approaches and tools, resulting in robust and consistent analysis and investigations which give management full confidence. This also facilitates the sharing of lessons across the sector. Most of these tools are suitable for use when investigating risk events and we have recommended three for adoption: Five Whys; Fishbone/Ishakawa; and Bowtie. Many of the organisations interviewed recognise that moving from a relatively ad hoc approach to investigations to a more systematic approach centred on proven tools is a quick win.

- **Become a learning organisation**

  World class operational risk managers supplement data from their risk event reporting process with data from other areas of the organisation and external risk events. There is an opportunity for many insurance companies to use more data from ORIC reporting across the sector to supplement internal learnings. Using external data helps businesses to create a culture of 'vulnerability and challenge' where all staff are actively conscious of potential risk events that may occur and proactively strengthen operational risk controls. In addition, best practice organisations use their learning actively to target year-on-year reductions in operational risk losses.

Maturity Diagnostic

	Reactive	Compliant	Proactive	High reliability
Open environment for reporting	• Only significant loss events are reported • Lack of leadership involvement • Inconsistent reporting processes • Fear of blame/ reprimand impedes reporting • People are unsure what to report and why • Reporting delegated to the 2nd line • Near misses not reported	• Coherent process for people to report loss events • Most events reported • Key people are risk aware • Key people understand how to report a risk event • Little focus on near miss reporting	• Everyone feels encouraged to report risk events • Simple standardised company-wide approach to reporting • Ownership of reporting at 1st line • Selected staff at 1st line of defence staff are focused on risk • Staff understand the need to report near misses. >50% are reported	• Single, simple approach to capture enterprise-wide risks • Everyone understands the current and potential risks they face • Everyone understands the need to report risk events and do so directly • Open, learning culture sees events as an opportunity to improve • Near misses actively reported in order to reduce frequency of loss events
Risk event analysis, investigation and impact assessment	• Focus on addressing recovery from loss events • Leadership seek to identify responsibility and blame • Root cause analysis (RCA) not conducted	• Root Cause Analysis (RCA) conducted for priority events • Focus on controls, processes and systems – not behaviours • Ad hoc and inconsistent approach to RCA - few standard tools • Little trained investigative capability	• Clear thresholds for Root Cause Analysis (RCA) • Standard, proven tools and approaches used to conduct RCA • Behavioural root causes always sought • Strong trained capability to conduct RCA • Top leadership reviews causes of major events	• Deep Root Cause Analysis (RCA) for key loss events and major near misses • Analysis identifies trends and causes from high volume minor events • All leaders are seen to engage in RCA • Focus on behaviours (why people acted that way) • Leadership, behavioural and cultural issues confronted • Quality assurance of investigations through peer and 3rd line review
Action management	• Actions for most loss events are not monitored or followed up • Follow-up for major events is on ad hoc basis	• Actions often derived so that they can be delivered rather than make a difference • Actions are managed, monitored and closed • Approach and tools for action management are not consistent across company	• Actions derived to make a difference • Actions are prioritised based on resources available and risk appetite • Actions clearly tracked and only closed on evidence • Top leadership review actions for major events	• Action management process integrated into company-wide continuous improvement approach • Actions may involve replacing existing controls that are not cost effective, not just adding additional controls
Learning and continuous improve-ment	• No systematic approach in place to learn from internal or external risk events • Learnings tend to be ad hoc and rely often on informal networks	• Changes to policies and procedures occur in response to significant internal risk events • Learnings not always shared across all relevant parts of the company • Review of major external loss events is not systematic	• Processes in place to prioritise and share learnings across the company from internal risk events • Learnings are derived from external risk events • Appropriate ORIC data shared with 1st line • Multiple channels used to engage staff in learnings • The 3rd line review learning effectiveness	• Learnings from loss events and near misses used to deliver year on year reductions in risk exposure • Rigorous approach optimise behaviours and controls based on learning from internal and external events • Proactive sharing and learning across the industry to reduce sector-wide operational and reputational risks

GLOSSARY

During the study, we noted there was some variance in the language used to describe elements of operational risk management. To assist with clarity, we have defined below some terms used in the report.

Analysis of event	The actions taken after a risk event to determine the root causes, assess the impact and identify potential remedial actions. Analyses can be focused on single events or groups of events to identify trends.
Chronic unease	A term used extensively in the asset intensive industries to describe an organisational state where people are highly risk aware and continually assessing what might go wrong.
Insurance sector	This includes insurance, reinsurance and asset management activities.
Investigation of event	To analyse the root cause/s of a major event, a formal investigation is often set-up. A dedicated multi-skilled team may be appointed to carry this out.
Risk event	An event that results in a loss event, fortuitous gain or near miss.
Loss event	An event that results in a financial and / or non-financial loss.
Near miss	An event that did not lead to a financial and / or non-financial loss, but had the potential to do so.

SCOPE OF THE REPORT

'Creating value from risk events' is a report which provides key insight and practical benchmarks to guide ORIC members and the broader industry in their approach to operational risk management.

It is illustrated throughout with best practice examples and learnings from within the insurance industry and other sectors, including mining, utilities, banking, oil and gas, aviation and public sectors.

Definitions and glossary of key terms

During the study, we noted there was some variance in the language used to describe elements of operational risk management. To assist with clarity, we have defined below some key terms used in the report.

Analysis of event	The actions taken after a risk event to determine the root causes, assess the impact and identify potential remedial actions. Analyses can be focused on single events or groups of events to identify trends.
Chronic unease	A term used extensively in the asset intensive industries to describe an organisational state where people are highly risk aware and continually assessing what might go wrong.
Insurance sector	This includes insurance, reinsurance and asset management activities.
Investigation of event	To analyse the root cause/s of a major event, a formal investigation is often set-up. A dedicated multi-skilled team may be appointed to carry this out.
Risk event	An event that results in a loss event, fortuitous gain or near miss.
Loss event	An event that results in a financial and / or non-financial loss.
Near miss	An event that did not lead to a financial and / or non-financial loss, but had the potential to do so.

Our study

28 ORIC members were interviewed to identify leading practice in risk event management, focusing on reporting, analysis and learning. In addition, four companies from other sectors (oil and gas, utilities, aviation and mining) were interviewed as comparators. From this, best practice approaches were identified and a maturity diagnostic developed to assist organisations in benchmarking and improving their performance. These approaches and the maturity diagnostic have broader applicability across other industries and sectors.

This document is not intended to prescribe particular methodologies. Each individual organisation will be faced with different scenarios, challenges and risks and the people working within it will need to use their own judgement to identify appropriate practices.

INTRODUCTION

THE IMPORTANCE OF EFFECTIVE RISK EVENT MANAGEMENT

Operational risk events have resulted in huge losses and reputational damage across all industry sectors. For example, BP faces losses of $43bn as a result of the Macondo disaster; the banking industry has had to pay out tens of billions of pounds in fines and compensation as a result of LIBOR, money laundering, mis-selling and other risk events; and public sector organisations like the NHS have suffered massive reputational damage around patient safety operational risks.

The insurance sector also endures large losses each year from operational risk events, often associated with significant reputational damage. In addition to impacting the P&L directly, capital reserves must be set aside to cover these risk events, which can have a significant impact on corporate return on capital.

Organisations which place a strong focus on risk event reporting, analysis and learning actively reduce operational risk losses. Typically, they exhibit the following characteristics:

- An **open culture** where people see risk events as an opportunity to improve
- Undertaking analysis of risk events to **understand the root causes** and establish whether other areas of the organisation could have an exposure
- A **disciplined** approach to deciding on management actions required in response to a risk event and their implementation
- Continuous improvement of their control framework using **learnings** from internal and external risk events to reduce operational risk exposures.

When an organisation gets these things right, it tends to outperform the market financially.

Six steps to successful operational risk management

In order to achieve the four characteristics described, we have identified six steps adopted by best practice organisations, which should be followed when managing risk events (see Figure 1):

1. **Identification of the risk event:** Determining that a risk event has occurred.
2. **Escalation:** Communication of the event to the appropriate parties.
3. **Event capture:** Detailed collaborative investigation of the root cause of the risk event to understand the actions which need to be taken to prevent re-occurrence.
4. **Impact capture:** Evaluation of the actual and/or potential financial and non-financial impact of the risk event.
5. **Event action monitoring and closure:** Efficiently monitoring and managing the delivery of identified actions for consideration; for inclusion in the Internal Audit or Compliance monitoring schedule.
6. **Learning and continuous improvement:** Regularly capturing and sharing learnings from internal root cause analysis and external risk events, including facilitating improvement of the controls in place to minimise risk exposure.

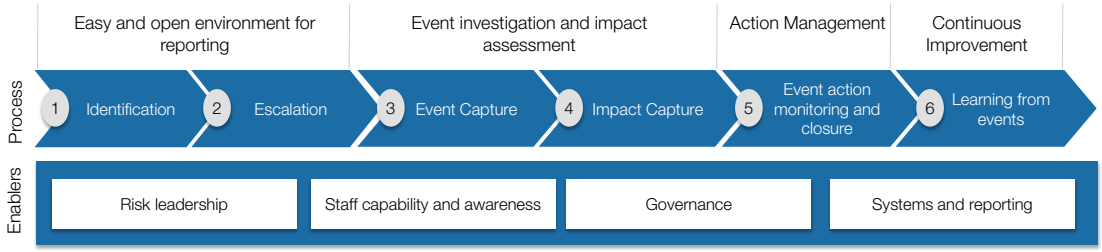


Figure 1: The risk event management approach

Enablers to effective process

ORIC has identified four specific enablers which are essential to the effectiveness of the risk event management process (see Figure 1):

1. Risk leadership

Leaders and managers at all levels:

- Have a thorough knowledge and understanding of risks and processes
- Actively champion and encourage a culture for staff to report risk events
- Create a transparent governance approach, so action owners are comfortable and empowered to report progress to an independent second line of defence team. This ensures delivery of satisfactory business outcomes.

2. Staff capability and awareness

All operations/first line of defence staff have good understanding of what a risk event is, how to report them and, where required, how to investigate them. This tends to be associated with detailed and simple guidance, supplemented with easily accessible support.

3. Governance

At all appropriate levels, diverse formal teams are in place to oversee risk event approach and performance. They have the influence to unblock barriers which reduce the effectiveness of the process, meeting at regular intervals to share learnings and address any trends impacting on risk performance.

4. Systems and reporting

At all appropriate levels, robust monitoring systems are in place, including summary indicators. This ensures consistency of approach and simplicity in managing and monitoring the risk event process, testing evidence to demonstrate an enhanced control environment.

RISK EVENT APPROACH

CREATING AN OPEN ENVIRONMENT FOR REPORTING

Transparency is key

An open culture enables organisations to have full transparent governance of risk events, maximising the opportunity to understand their risk profile, including identifying potential areas of control investment.

What does good practice look like?

An open culture and good governance has the following characteristics:

- People are incentivised and feel valued and respected when reporting a loss event or near miss without fear of blame
- The reporting process is as simple and user-friendly as possible
- All people are clear on their role in risk management and how to report risk events because they have access to easily accessible, unambiguous, jargon-free guidance
- People see the value of reporting for them and for their organisation
- Communication of events is timely and efficient, particularly in high priority cases.

Leading practice organisations recognise that robust processes and supportive monitoring systems are essential to encourage staff to report. However, they also recognise that effective reporting also requires strong and supportive leadership, staff awareness and understanding, and governance.

The vital role of leadership

The absolute key to achieving an open culture and good governance is visible leadership behaviour. Best practice organisations have strong, risk-aware leaders who actively champion the process, get involved in training staff, communicate the importance of risk to the business, actively follow-up on actions, and recognise staff for reporting. Such organisations invest in developing risk leadership skills and measuring leaders' performance in this area. Critically, these leaders avoid blaming those who report, or those who have made genuine mistakes, and place a high value on the opportunity to learn from events to improve the business.

Typical leadership interventions:

- Communicating at all relevant engagements that 'reporting is an opportunity for the business to improve'
- Continually emphasising that there is no 'blame culture' for reporting:

  > An insurer had an issue in the early stages of its risk management journey, when a senior executive discouraged reporting as he felt highlighting risk events in his business area made him 'look bad'. After the CRO made it clear that staff reporting these events would be protected from repercussions, people began to challenge management, insisting risk events must be reported even if they did not like it.
- Communicating the message that 'it is better to report in the first instance, rather than the unreported event being revealed later'
- Recognising people for reporting - good examples include publicly thanking those involved and/or thanking them personally:

  > At one oil and gas company, the CEO makes time in large all-staff meetings to acknowledge those who have reported, congratulating them and providing small monetary rewards
- Personally following up on actions which are overdue:

  > The CFO of a large insurer actively follows up on business units which are sending nil returns or reducing levels of reported events, asking why, and how they can help to ensure staff are fully aware and able to report.

Leading example

Flying operations on a nuclear carrier involve the most complex and risky of operations. Yet the most junior sailor on the flight deck is empowered to stop flying operations if they perceive there is a safety risk. In a recent risk event, a sailor stopped flight operations because he had mislaid a tool and was concerned it might have been sucked into the engines of a fighter aircraft. After a search for the missing tool had begun, he discovered it in his tool bag. Far from being reprimanded for carelessness, the seaman was publicly congratulated by the commanding officer for his risk awareness and taking the correct steps.

Organisational roles and governance

It is important for all staff across different levels of an organisation to be involved in reporting risk events, not just the second line of defence. In organisations which are in the early stages of their journey towards improved operational risk management, or those which are relatively small, the most effective approach may be to designate a risk champion or co-ordinator in the appropriate business area, who can help staff to fully capture the detail of risk events which occur.

Business and group risk committees can review the risk events and provide support to the risk owners to ensure mitigation is adequate, actions are being closed and learning is being shared across the business as a whole.

Staff understanding of risk events

People must understand what constitutes a risk event so they know what to report. For example, the event they are faced with could be a boundary risk, such as an underwriting risk, rather than an operational risk - they should know the difference. Nevertheless, if in any doubt, the risk event should be reported to the second line who can make a judgement.

In one example provided in interview, the telephone system of an organisation failed and the member of staff who identified the problem did not consider this to be worth recording, even though it impacted on the company's ability to transact and ultimately its reputation.

Near miss reporting

Many organisations find it difficult to create a strong and consistent level of understanding among their people of what a near miss is and why it should be reported. As a result, near miss reporting can be minimal. Best practice organisations focus heavily on near misses so they can address control or behavioural failures before they result in actual events and losses.

Hidden near misses

A mining company has focused for two years on near miss reporting as a means to reduce the number of actual risk events. It reported 1,870 near misses last year, against 840 actual events. Even so, the company believes only 60% of near misses were reported as opposed to more than 95% of actual events.

Getting everyone on board

Organisations with the highest rates of risk event reporting work continuously to engage with staff at all levels, and invest in building and sustaining staff awareness and capability.

Engaging staff through training

Typical training interventions include:

- Incorporating risk awareness and reporting training for all new staff through corporate induction programmes, and future leaders through development schemes
- Running a compulsory annual training module for all staff, including the leadership team, relating to risk management and reporting:

  One insurer has used situational training, giving staff risk scenarios and asking them to consider if they should report them or not.
- Providing very simple guidance notes on the intranet site, alongside the risk reporting system.
- Ensuring there are 'risk champions' within the first line business area who have a strong understanding of what should be reported and how. Personal reviews and annual target evaluation of business risk champions could include input from the Risk team on the quality and timeliness of event source data.

The loss event and near miss reporting system

ORIC has identified five common steps that leading practice organisations follow to report a risk event (see Figure 2).

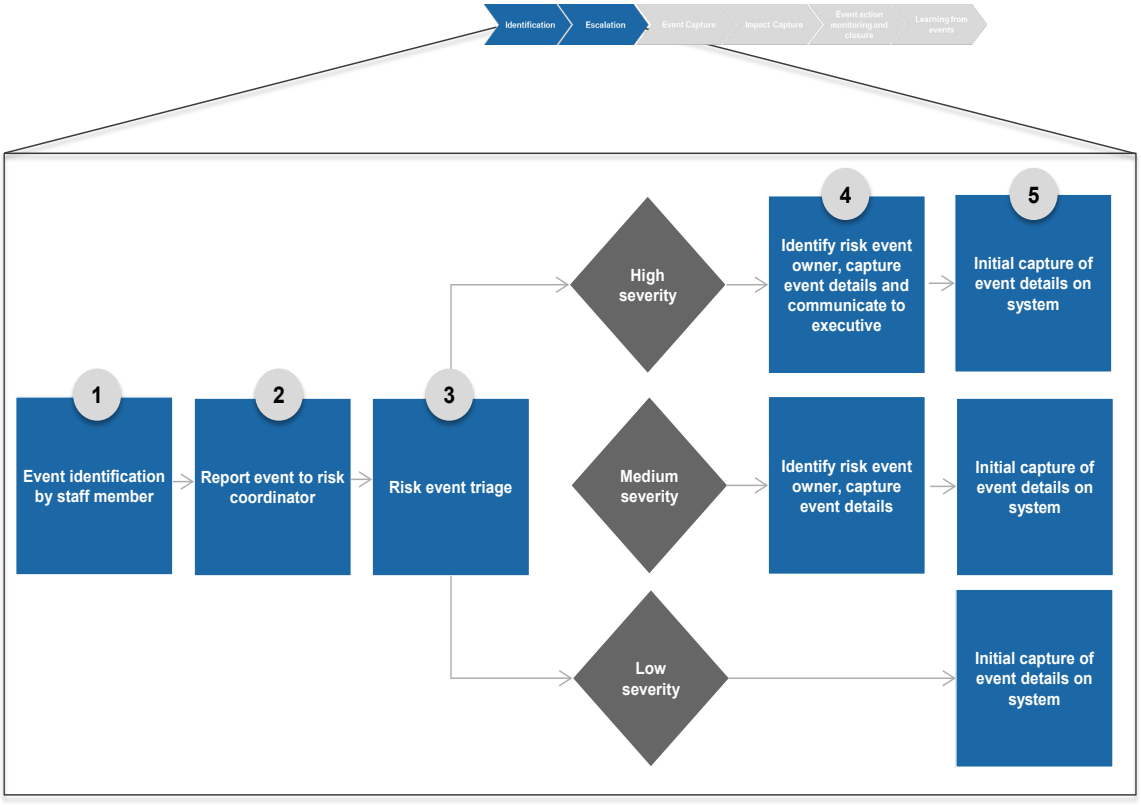


Figure 2: Risk event reporting process

Key roles

Risk champion/co-ordinator: A member of staff in the first line of defence who is responsible for risk management in the relevant business area.

Risk event owner: A leader in the area where the impact is felt and/or where actions are taken. This person should be assigned ownership of the event and its follow-up. Where multiple areas of the business are impacted, the Risk team may lead the initial review, with ownership transitioning into the business on identification of a suitable leader or leaders (for example, from a business area or business areas that have the greatest impact or has the most significant remediation activity).

Research report

Step	Activity	Timing	Responsibility
1	Event identification: All staff must understand and be able to identify the following: • An actual loss event • Potential risk event (even when a loss has not yet been identified) • A near miss (e.g. a control failure). In any event, the principle of 'if in doubt, escalate' should be applied. For frontline staff, there are advantages in having no threshold for the capture of events. This will avoid any doubt about what to report and also ensure that small loss events are recognised as potential larger near misses. An event must never be considered out of scope because of perceived sensitivities.	On identifying a potential or actual risk event	All staff
2	Report event On identifying an event, staff should report a high level description of what has occurred to their local manager or risk champion or co-ordinator. This can be a simple call, email or note, stating the following: • Date of the event • Description of the event • High level financial and non-financial impact • Issue identified by/method of discovery. Sensitive commercial and litigation issues may require special handling.	On identifying a potential or actual risk event On identifying a potential or actual risk event	All staff
3	Risk event triage: Based on analysis of the event, the risk champion/co-ordinatorshould estimate its severity, based on financial and non-financial impacts and potential impacts to the business. The following matrix can be used to determine the severity: • High: A major event or near miss which needs to be brought to the attention of top management without delay, based on size and/or reputational impact • Medium: A significant event which requires corrective and/or recovery action based on size • Low: A minor event which should be addressed locally, but must be reported for quantification and trend analysis.	Immediately on hearing of the potential or actual risk event	Risk champion/ co-ordinator
4	Medium and high severity actions: If the severity of the event is defined as 'medium' or 'high' then a risk event owner should be assigned ownership of the event and its follow-up. The event owner, working with the second line of defence, should assess the severity of the event and associated actions: • High severity: Verbal event escalation immediately to the CRO/a group executive member and the second line of defence • Medium severity: Verbal event escalation not required. The second line of defence should support and, as required, challenge the event owner in capturing all the details and communicating the event in the escalation process. (See following example of template for communication to the executive)	Within 24 hours of risk event being identified	First and second lines of defence

5	Initial capture of event details: For events classified at any severity level, the following details should be captured and submitted on the risk system: Details: • Severity level • Event status • Event owner • Business unit/area • Date of event impact. Event details: • Description of what happened • Primary and secondary causes (based on ORIC definitions) • Estimated impact • Currency • Estimated/actual impact • Non-financial impact • Category of impact. Actions taken: • Detail/classification of actions • Owner of the actions • Date on which actions were allocated • Completion status • Target date.	To be completed within two working days of the risk event being identified	Event owner or champion/ co-ordinator

Choosing the right reporting system

An organisation's front-end reporting system should be on an easily and commonly accessible and user-friendly platform - typically via the company's intranet site.

There are different models of reporting systems which reflect different corporate environments. For example:

- A global company with a major UK division may use different systems for separate geographical regions to reflect different regulatory requirements
- In very large companies, most operational risk management can be carried out with relatively 'light touch' management at group level, again reflecting different regulatory models
- For the smallest companies, where staff number in the low hundreds, and where there are strong personal contacts across the business, email and spreadsheets may suffice.

There are significant advantages in having a single, enterprise-wide risk reporting system which covers, not just all divisions, but also key outsourcing providers.

One insurer is currently transitioning the systems it uses internally with all its outsourcers, so the language and terminology is the same.

The cost of poor reporting culture: Mid Staffordshire NHS Foundation Trust

Some 1,200 unnecessary patient deaths occurred over a period of years at the Mid Staffordshire NHS Foundation Trust hospital, the causes of which were initially ignored. On initial investigation, these were attributed to a variety of causes, including lack of cleanliness, nurses being overloaded with work, lack of supervision, hospital bugs, and so on. A recent report by Robert Francis QC identified two much deeper root causes:

- A ruthless prioritisation of financial performance over patient safety was imposed from top management
- A closed, blame-laden culture existed, where people at all levels were frightened to speak out.

NOTE: The qualitative event narrative should:

- Be written in plain language, be free of jargon and have any acronyms defined on first appearance. If a system name must be used, make it clear what the system does and its importance to the organisation
- Contain no sensitive information, such as reference to customer, employee or third party names
- Exclude comments which might be considered inflammatory or defamatory.

Example: High Severity Event Template

This template is used by one organisation to escalate a major risk event to top management.

CONTENT:

1. Event title: Provide a brief title for the event, linked to impact or control. Where an event is a recurrence of a historic issue, this should follow a similar title to allow the reader to understand the link.
2. Dates: State the date the event was discovered and the date on which the event occurred.
3. Impacts: Provide details of all actual/potential financial impacts and/or non-financial impacts, ie. customer, regulatory.
4. Causes: Provide a clear description of the root cause(s). If not known, include a sentence to explain the status of any investigations in progress.
5. Rationale for escalation: State the purpose for escalating. This should include the nature of the event, the event type, actual or potential loss/gain and geographical location.
6. Immediate actions: Provide brief but clear details of actions which are being or will be taken; include whether risk event management is invoked.
7. Other need-to-know facts: Include reference to any regulatory notification issued.
8. Business or support function executive: Provide the name of the executive or member of senior management who will own this event.
9. Contact: State the name, email address and full telephone number of a member of staff who can be contacted for further information.
10. Timeliness: Provide an appropriate explanation if the escalation is beyond 24 hours following discovery.
11. Enterprise Risk Policy Framework: Provide an indication of the appropriate minimum standard that the event will be mapped to, in order to support reporting.

EVENT INVESTIGATION ANALYSIS AND IMPACT ASSESSMENT

Objectives

Effective risk event analysis and investigation ensures the business fully understands the root causes of each significant risk event, determining the most appropriate mitigation actions to minimise the risk of re-occurrence. Building on the understanding of the root cause, it also captures the financial and non-financial impact of the loss event (or potential impact in the case of a near miss) to allow recovery actions and to quantify overall losses.

Understand the reasons why

With a few exceptions, most insurance companies use a relatively ad hoc approach to analysing the root cause(s) of significant risk events. While this approach allows flexibility to tailor approaches, a base level of standardisation instils business discipline. Other industries use proven industry-wide approaches and tools, resulting in robust and consistent investigations which give management full confidence.

It is easy to blame a system or human error for a risk event occurring. But it is critical to understand why someone made a decision. The two main causes of people not following process in the insurance industry are reported to be:

- A lack of awareness, training or understanding
- An active decision not to follow process. The underlying cause of this is often the prioritisation performance over risk management, which itself may be the result of the tone set by top leadership.

The second of these causes may be a reflection of the perception of the priorities afforded by the organisation to driving performance as opposed to managing risk. Management decisions to take a particular course of action, even if on the face of it perverse, are seldom malign. Leadership must consider carefully how the tone they set may be interpreted by front line staff.

The impact of a risk event is also frequently overlooked, particularly when not classed as a 'major' loss event. Without this data, a business may not pick up key systemic failures which could appear minor when taken individually, but in aggregate be significant, with a large non-financial impact (e.g. reputational damage).

An insurance company found that, on a number of occasions, it had sent incorrect statements to its customers. This was not captured as a risk, as there was no financial impact directly associated with the event. However, a serious risk event did occur later with the same root cause, resulting in the organisation refunding a large amount of money as compensation.

Behaviours matter

27% of risk events reported to ORIC list the primary cause to be people related. More broadly, Oliver Wyman research across the whole financial services sector shows that over 60% of risk events are related to people issues, but less than 10% of mitigation initiatives relate to behaviours. Without appropriately addressing behaviours, organisations typically risk repeating the events in the future. Deep root cause analysis in other sectors, particularly where safety is involved, has a major focus on people issues, culture and behaviours.

Characteristics of good practice

A robust root cause analysis and impact assessment approach has the following characteristics:

- Clear thresholds when deep root cause analysis of risk events is required
- The root cause(s) of a risk event is thoroughly investigated, with a balanced focus on people and related skills; capabilities; culture and behavioural issues; processes; and systems
- Investigation of significant risk events is carried out by a combination of first and second line staff, who have investigative expertise and appropriate professional skills, working closely with first line subject matter experts
- Quality assurance is in place to ensure investigations are conducted to a certain standard
- The risk event data is back-tested with the P&L to provide assurance
- Risk events are compared against the relevant standard or policy, with weaknesses identified and prioritised
- Trend analysis of operational risk events are identified to support strategic improvement of controls, processes, systems and behaviours.
- All risk events have associated with them an actual or potential financial or non-financial impact.

The root of the issue

All risk events require some level of root cause analysis. However, deep root cause analysis is a resource intensive process, so assessing the severity of the event is key in determining the level to which it should be investigated. For events classed as low severity, the simple root causes can be identified by local teams, using a standard template which may be accessible on the risk reporting system. For the more systemic and complex medium and high severity risk events, leading practice organisations use deeper root cause analysis tools.

When to use root cause analysis

Root cause analysis should be used:

- In medium and high severity cases
- For reoccurring events
- For events occurring regularly, where multiple areas of the business are involved (e.g. when repeated claims are impacting on customer services)
- When certain infrequent events have a wider impact (e.g. underwriting errors).

When not to use root cause analysis

Root cause analysis is not necessary for:

- Low severity risk events. This does not of course mean ignoring large groups of related small issues, but rather ensuring that the root cause analysis process does not become over used because it is too costly to start or maintain
- Single events where the cause is clear and there is no appetite to deploy resources to investigate: e.g. ‘Acts of God’ impacting your business where all controls and actions performed as expected.

> Best practice is to set clear thresholds above which full root analysis is required. These thresholds should include non-financial (e.g. reputational) as well as financial impact criteria.

People pointers

- Ensure that selected staff are trained in investigating risk events using root cause analysis tools - eg. risk champions/co-ordinatorsin operations; risk professionals at second line; or other second line of defence teams (eg. Information Security or Compliance).
- An appropriate balance of responsibility should be assigned between first, second and third line staff. It is important to conduct rigorous and independent investigations, without losing front line ownership of the problem.

An insurer has appointed risk owners for each of the 30 major risks and procedures used in their insurance operations. When a risk event occurs, these owners act as subject matter experts to challenge and support the first line ofdefence, so the investigation is robust and actions are appropriate.
They can then update policies so the business adjusts its processes to reduce the likelihood of re-occurrence.

During major investigations at an oil company, an operational team from a different business area, which faces similar challenges, is brought in to peer review the investigation process and outcomes. This also helps to spread best practice between business areas.

Setting up a root cause analysis (RCA) forum

A large retail insurer has established a RCA forum to help co-ordinate, centralise and govern all RCA activity. The monthly forum is made up of representatives from a broad cross-section of the business.

This RCA forum is responsible for:

- Agreeing topics and issues to focus on:
  - Ensuring the RCA process is conducted in a robust manner
  - Reviewing the output of the RCA process
  - Reporting findings to the executive
  - Ensuring the actions from the RCA are prioritised and implemented
  - Reviewing the performance and impact of the changes implemented.

Recommended best practice

ORIC has developed a six step process to investigate and analyse the details of a risk event and its financial and non-financial impact (see Figure 3).

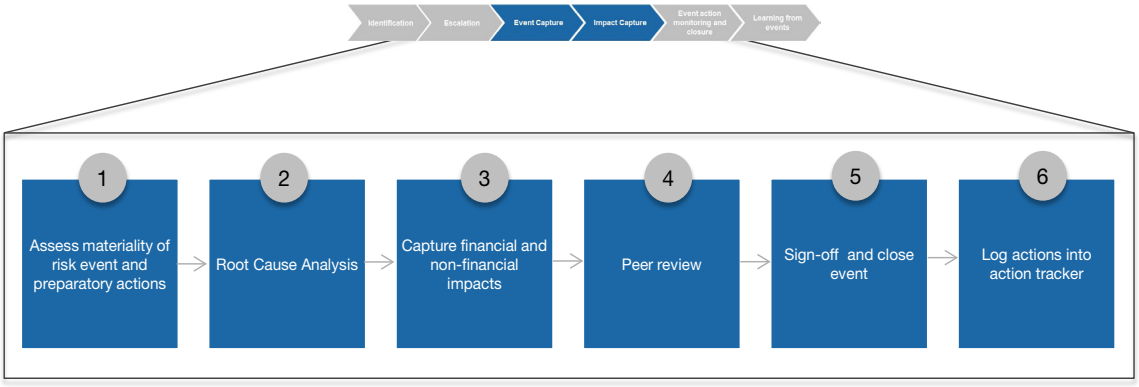


Figure 3: Capturing risk event information and impact

Step	Activity	Timing	Responsibility
1	Assess materiality and preparatory actions: • Event owner assesses materiality of risk event • Event owner assess skills and capabilities required for the investigation • Event owner is responsible for assembling the appropriate team to investigate the risk event, and agreeing its scope • Members of the team can include the process owner, second line of defence, SMEs and line management. It is preferable that the process is not led by the second line of defence.	As soon as possible after risk event is identified	Event owner
2	Root cause analysis: 1. Understand the problem: • Gather information about the risk event, considering influences both inside and outside the end-to-end process • Review the current business controls and thresholds • Determine what the standard process is and identify what 'good looks like' • Capture details of what actually happened. 2. Identify the root cause: • Apply root cause analysis tools (see below for details) • Prioritise and identify the key root causes. 3. Recommend solutions: • Develop actions and a plan to address the root causes of the event • Determine the financial costs and ease of implementation of the actions. • Validate proposed root causes with all parties involved.	As soon as possible after risk event is identified	Event owner
3	Capture of financial and non-financial impacts (actual or potential): • See Figure 4, 5 and 6 for a list of direct, in-direct and recovery categories.	Immediately - for high level estimation of impact, then obtaining more detail when possible	Event owner

4	Peer review: • Produce and present report to the RCA team • Where appropriate, validate the findings with a similar team in a different business area.	Once all other steps are completed	Head of business area/ second line of defence
5	• Once all other steps are completed.	Head of business area/ second line of defence	Head of business area/ second line of defence
6	Log actions on actions tracker: • Log actions on the appropriate system for implementation.	Following closure of event investigation	Event owner

Root cause analysis tools

Few insurance companies interviewed use proven standard tools for root cause analysis, exceptions being two companies who use Five Whys. Some companies use a customised approach embedded in their own reporting systems; and many rely on an ad hoc approach.

There are a number of proven standard tools of various levels of sophistication which have been developed in other sectors, often for use in asset intensive industries. The simpler of these tools include the following, which are recommended for the insurance industry:

Five Whys: getting to the deep root cause of simple, linear events - Appendix 1

Fishbone diagram/Ishikawa diagram: a simple but robust approach for investigating relatively simple events - Appendix 2

Bowtie: a more sophisticated tool which can be used across scenario planning, investigation, decision making and communication - Appendix 3.

Impact analysis

The ready reckoner tools below at Figure 4 and 5 can be helpful in ensuring all aspects of the risk event are analysed.

Impact	Result
Compensation impacts	Ad hoc payment
	Charge and fee waiver
	Soft-dollars
	Compensation payment
	Premium discounts
Legal impacts	Court-ordered settlement
	Out-of-court settlement
	External litigation fees and costs
	Internal litigation fees and costs
	Litigation settlement
External direct impacts	External advisor costs
	External remedial resource costs
Internal direct impacts	Internal overtime paid
	Internal remedial costs
	Increased operating cost or cost of control

Regulatory impacts	Fines
	License suspension
	License revocation
	Direct regulatory sanction impact
Direct financial impacts	Loss or damage to assets (including write-downs)
	Debt write-offs and write-downs
	Loss of recourse
	Restitution
	Unexpected gain
	Other P&L loss impact
	Other direct economic write-offs and write-downs
	Net interest settlements
	Gross interest settlements
	Assets stolen
	Unbudgeted costs

Figure 4: Financial impact categories

Impact	Result
Indirect regulatory impacts	Indirect regulatory sanction impact
	Indirect license revocation impact
	Indirect license suspension impact
Indirect financial or accounting impacts	Capital account impacts
	Public misreporting impacts
	Excess dividends
	Share price impacts
	Indirect revenue impacts
	Preliminary economic estimates
	Preliminary timing estimates
Indirect external impacts	Ratings downgrade
	Costs of external repair or replacement
	Reputational impacts
	Health and Safety impacts
Indirect internal impacts	Staff opportunity costs
	Bonus payments to employees
	Business opportunity costs
	Other indirect impact

Figure 5: Non-financial impact categories

As part of the input analysis, it is important to consider and capture recovery actions which can be offset against the loss. These should be reported separately and not netted off. Figure 6 below suggests some recovery categories.

Recovery categories
Other insurer recovery
Client repayment or recovery
Third party recovery
Reinsurance recovery
Government or state recovery
Salvage or scrap sales
Insurance recovery
Use of funds

Figure 6: Recovery categories

Final event report

The final event report can be completed once the root cause analysis and impact assessment are complete. ORIC recommends that it should include the following detail:

Risk event details:

- Risk event title: concise description of the risk event, highlighting key points
- Event recognised date: The date when the event was discovered by the member firm
- Event occurred date: The date when the event which gave rise to the risk event happened
- Business area that gave rise to the loss
- Business area/s impacted by the loss
- Risk event description
- Risk event classification
- Status: Open/Closed
- Geography: The country or region where the risk event occurred
- Cause description: Description of the root cause/s of the event
- Causal classification.

Impact breakdown

- Near miss/actual loss
- Gross loss
- Recovery
- Reputational impact
- Other.

ACTION MANAGEMENT

Objectives

The objective of action management is to implement agreed activities to recover from the event itself and to reduce the risk of re-occurrence. It is used to find the appropriate balance between potentially conflicting objectives, ensuring all significant actions are carried out, and avoiding the imposition of an unwieldy bureaucracy.

An organisation can suffer from being overloaded with actions. This typically not only reflects how the organisation values the importance of risk, but also illustrates how operationally disciplined it is continuously to improve more generally.

Good practice characteristics

A strong action management approach is in place when the following exists:

- Transparency of the progress and closure of all critical actions arising from the reporting and analysis processes
- Established KPIs to manage the performance of the business in completing the actions
- Appropriate governance to monitor issue implementation of actions at local, divisional and group level. This must have the necessary influence to unblock issues which impact delivery
- A robust approach to prioritising actions, aligned with the organisation's defined risk appetite, to ensure that limited resources are focused on the most important controls and barriers.

Stages in action

ORIC has identified three key stages in the action management process (see Figure 7):

Stage	Activity	Timing	Responsibility
1	Review and prioritise actions: 1. All action owners provide a progress update to the risk owner on delivering the actions. 2. The second line of defence reviews the actions to ensure the quality of the information and, if required, provides challenge back to the owner. 3. Following the organisation's standard change control methodology, the relevant risk forum should review the following: • All medium and high severity open actions, timings and notes on progress and issues • Overdue actions • Resources available to close actions • How the critical actions will be delivered and, if required, what action is necessary to remove blockers to implementation • Escalation of critical actions to executive risk committee or relevant forum where required • Agreement of which actions not to pursue based on the organisation's risk acceptance model and cost-effectiveness.	Monthly	Regional, Group Risk committee, or similar risk forum
2	Deliver: • Implement the agreed action.	As required	Action owner

3	Complete actions and sign-off: • Update the action tracker with information regarding the outcome and news that the issue has been resolved • Second line of defence reviews the actions, identifying evidence that the action has closed and it has effectively resolved the issue • Second line of defence closes the event off on the system.	On completion of all relevant actions	Event owner

Figure 7: Stages of action management

Systems and reporting

It is preferable to have a single database to capture all actions across the business. This will help in achieving consistent oversight of each business and in ensuring delivery is robust. The database should be accessible to the action owner or control performer in order to continue to provide regular progress updates. In larger organisations, the database will be automated. The second line of defence should be able to produce reports as input to the relevant risk forums.

Targeting timely action

One insurance company has a target of no more than 10% of action items overdue. If actions become overdue then exceptions are reported to the risk management committee, which reviews and challenges business owners to deliver on time or to reprioritise actions.

Priorities of leadership

Leadership must ensure that actions arising from risk events are appropriately prioritised and not subordinated to 'business as usual' activity. However, the risk management process quickly becomes discredited if the business aims for a 100% closure rate for all risk actions regardless of priority and cost effectiveness.

> One particular organisation explained in interview its policy to close all actions within 30 days. If the action was overdue, this would be reported to the CEO. This created a culture of fear and drove the business away from considering the real priorities resulting in resource not focused on the overall business priorities. It is critical that appropriate pragmatism exists so, if an organisation has a lack of resource to deal with the number of risks it faces, then it has a robust risk acceptance model preventing resource being consumed in low priority actions.

Risk acceptance

A large global insurer has many more actions identified than it has resources available to impact them. It prioritises against cost-effectiveness and its risk acceptance model. The company classifies all its actions as RED, AMBER or GREEN to illustrate if deadlines have already, or are expected to be, missed, and use the 'acceptable risk' approach to manage out low priority risk actions.

Driving quality in follow-up

A large global retail insurer focuses on the quality of its follow-up actions to avoid a 'box-ticking' approach. This is achieved by:

- Challenge from the second line of defence and use of subject matter experts from other divisions
- Examination of outcomes rather than outputs
- Actions are only signed off by the second line if they are evidenced.

Roles and responsibilities

First line

It is essential that the risk event owner, usually a manager from the first line of defence, takes responsibility for actions following an event. The first line is best placed to make any changes as it will have control of the organisation's resource, along with accountability for operations.

Second line

The second line of defence is suited to providing challenge, support and assurance. Its role will often be to monitor that the first line risk event owners provide detail of their progress in implementing actions; to make sure the best approach is taken; and to identify and facilitate the escalation of issues or blockers that may exist. The second line should also focus on identifying trends relating to risk events, such as systemic issues which each business silo would find difficult to identify. They should highlight these to the relevant risk forum and propose appropriate actions.

Third line

The third line provides the assurance framework. It reviews the closure of actions and assesses risk scenarios to ensure their robustness.

Risk committees

Risk committees are key to ensuring any actions are monitored and delivered. As they are made up of senior business leaders, they assess, prioritise and dedicate resource, and are able to remove barriers in the way of implementing actions.

Managing outsourced operations

Leading organisations fully integrate their outsourced operations into their risk event management governance and approaches:

One insurance company manages several large outsourced operations. These outsourcers typically have a number of competing priorities when considering implementing actions associated with risk. To manage performance, outsourcers are assessed by the speed and effectiveness in which they close actions, using Service Level Agreements (SLAs) to hold them to account. If these SLAs are not sufficient to influence them, then, where required, other strategic initiatives are stopped to ensure the outsourcer has the resource to focus on closing risk actions down. One outsourcer proposed to move activity to India to reduce costs. A larger national insurer did not allow the move to take place until the outsourcer had closed down a number of their risk actions. This was enforced at senior executive level during monthly service contract management review meetings.

LEARNING AND CONTINUOUS IMPROVEMENT

Objectives

The value in learning from others

Following a risk event taking place in one part of the business, the learnings and actions taken could often benefit another part of the business. In addition, another company in the industry may experience a risk event and the learnings from this could help to strengthen the controls sector-wide, helping mitigate a future risk. Alternatively, a leadership team may become complacent due to no major events having taken place in the last few months and so begin to relax their focus and priority on risk, dedicating energies to other challenges.

Creating a culture of vulnerability and challenge

Effective learning from risk events not only helps to identify gaps in existing controls, but importantly helps create a culture of 'chronic unease'. This is an organisational state where people are highly risk aware and continually assessing what might go wrong, as well as being prepared to challenge processes and leaders from an informed basis.

The objective of the continuous improvement stage is to systematically reduce group-wide risk exposure by efficiently and effectively learning from risk events occurring both within and outside the business. Learning also helps create the necessary culture of 'chronic unease' described above.

Many organisations struggle with this phase as they are busy dealing with day-to-day challenges. However, those which do have a good approach tend to be risk leaders in their industry.

Leading practice characteristics

An organisation which systematically and continuously improves does the following:

- Set targets to reduce annual operational risk exposure using financial and non-financial targets
- Captures learnings from internal risk events
- Captures learnings from appropriate external risk events
- Has an effective process to prioritise and target learnings, with the appropriate channels and techniques to effectively communicate and engage the appropriate staff in these learnings
- Has a continuous improvement culture where the business is in a state of 'chronic unease' - looking for opportunities to strengthen its risk knowledge and controls.

Route to continuous improvement

ORIC has identified four major steps in the continuous improvement stage (see Figure 8):

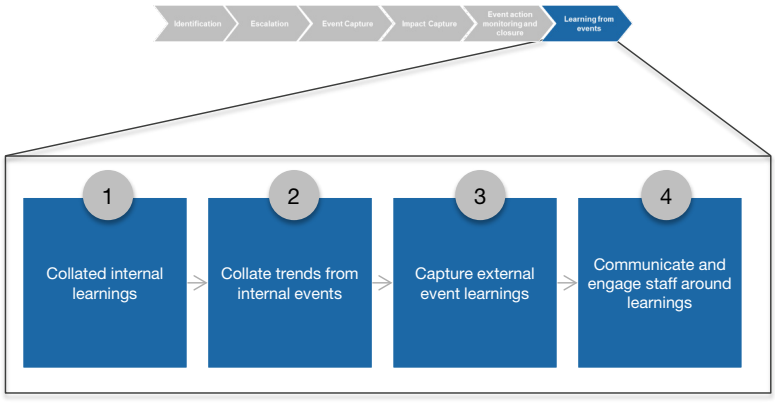


Figure 8: Steps to continuous improvement

Step	Activity	Timing	Responsibility
1	Capturing internal event learnings: 1. Collate information from all risk events occurring in the last month and identify key events which have value to be shared across the business. 2. Capture learnings from the selected events in a summary, covering: • Event description • Root cause/s of the event • Impact • How the investigation was completed.	Monthly	Second line of defence
2	Collating internal event trends: 1. Review all the events occurring in the last month and identify common trends, including: • Geographic/locational similarities • Root cause similarities. 2. Identify if any of the identified trends are not being addressed by the current set of actions in place (captured in the actions log). 3. Produce a summary presentation of any findings not being addressed by the current set of actions for review of the risk committee.	Monthly	Second line of defence
3	Capturing external event learnings: 1. Collate information from all external risk events occurring in the last month and identify key events which have value to be shared across the business or for specific businesses. 2. Capture learnings from the selected events in a summary, covering: • Event description • Root cause/s of the event • Impact • How the investigation was completed.	Monthly	Second line of defence
4	Communicate and engage staff around learnings: Produce a risk event presentation, or set of presentations, focused on the following three communities: 1. Cross-business: Share learnings in the appropriate format from key internal and external events across the business. 2. Risk community: Share detailed learnings from key internal and external events with the risk management community (including line managers, risk co-ordinators and the second line of defence). 3. Specific business areas: Share certain internal and/or external event learnings with specific business areas, and ask them to do the following: • Review the event details with the following question in mind: 'Could this happen to us?' • Report back to the risk committee that there are appropriate controls in place to mitigate the risk or detail the action plan developed in response, in order for the necessary controls to be strengthened.	Monthly	Second line of defence

It all comes back to leadership ...

Emphasise the importance of learning

It is a leader's role to create the space and time to focus on learning from risk events.

Many companies get caught in the trap of 'fire fighting' - reacting to short-term risk events - which means they feel they are not able to focus on events which may not have an immediate material impact. Becoming more proactive in learning from events will mean, in the long term, that the business does not have to make a mistake before it acts.

Recognise staff efforts

Aligned to leadership support, the organisations which are most successfully managing their risk events are also recognising staff for their ability to take on learnings.

One oil and gas organisation initially began offering gift vouchers to those who made an impact on the organisation, strengthening its controls. It supplemented this by recognising staff contribution, openly acknowledging their actions at staff meetings and conferences. They found this was more powerful than offering financial rewards.

In another organisation, in their personal balanced score cards, risk managers have included the need to incorporate learnings from risk events into their risk improvement plans.

Set targets and keep to them

Leading organisations are taking advantage of their ability to prove how they continuously improve their operational risk management controls. As a result they are able to evidence how the business can reduce operating costs through managing operational risk effectively. A number of organisations are setting targets to reduce annual total operational risk exposure, based on proving how they have strengthened controls and barriers in their scenario analysis process.

Sharing learnings from risk internal and external events

One global insurer takes several innovative measures to share its learnings from risk events

- The company creates a pack of risk events to share with the risk co-ordinators, who are expected to discuss the pack at their local risk meetings, and identify one or two themes for discussion
- Each quarter, a compendium of around 20 relevant risk events is compiled. A central risk co-ordinator then decides which parts of the business would benefit from access to the learnings and sends it to them. The target areas are then expected to review the risks and assess if their business adequately controls against them
- The company picks out one or two internal and external events to share in its monthly magazine. This publication usually follows a theme, with the events featured consistent with this, reinforcing the overarching message. For example, the last magazine concentrated on anti-bribery and the events shared highlighted related external risk events and their impact and consequences
- The business has a comprehensive risk training programme, with the alumnus receiving one-page documents of interesting risk events to keep the conversation going.

Sharing internal learnings

One insurer sends out one-page summaries of key learnings to relevant recipients and first and second line. An example is:

Risk Event no: xxx

- Description: Following a request for 'input' into a newly proposed service arrangement, technical specialists determined that 'indequate' controls had been established to handle the processing of personal data outside out company's direct control. As a consequence the possibilty existed that our company could have found itself in breach of the Data Protection Act.
- Consequence: Near Miss (if found in breach, potential FSA fine = £2,275,000)
- Contributing factors:
  - Lack of understanding of Data Protection Act compliance requirements
  - Failure to obtain proper legal advice regarding third party handling of personal data
  - Lack of awareness of company's Group Outsourcing Policy – ROOT CAUSE
- Proposed actions:
  - Communication of Outsourcing Policy to emphasis implications of information transfer and need for due diligence
  - Ensure Data Protection Act implications of working with suppliers are reviewed and understood
  - Revise current scheduling of Technical specialists' involvement in supplier tendering process – consider earlier involvement.

Sharing learnings from ORIC submissions

One insurer sends out quarterly reports to the risk function, and leaders and risk champions, summarising learnings extracted from ORIC data. Typically, 15 one-page summaries per quarter are created and sent out to relevant recipients at first and second line. An example is:

- ORIC Event 54031 – Pricing error
- Description: A system release created an error in an unrelated part of the system resulting in cases being underwritten with terms that were too generouse for the period that the error was in place
- Cause: Inadequate Software (coding/design/testing/legacy systems)
- Consequence: Loss £200,000
- Relevance to our company?:
  - Are there unknown dependencies in the systems used by more than one Function?
  - Are there controls in place to check how chnages or upgrades may impact other parts of our Underwriting systems?
- Have similar events occurred in our company?
  - In 2012 to date, there have been four events relating to the Inadequate Software (total £60,000 in losses)
- Function Affected: Group Acturial/Group Underwriting/Tech Specialists/Divisions

‘Could it happen to us?’

A global insurer uses a number of approaches to share risk event insights

- The company sends out a quarterly pack, tailored to specific monthly themes, to its risk community, highlighting the top five recent risk events, in order to illustrate trends and examine why the events occurred
- The second line of defence is sent ‘it could it happen to you’ emails based on high severity events with broad applicability. For instance, emails are sent to risk managers, who are required to confirm to the group function that they have accessed their controls and are comfortable the correct barriers are in place
- Trends analysis for the risk committee is regularly conducted.

MATURITY DIAGNOSTIC

From this research we have developed a maturity diagnostic that covers the four areas of loss event management that we have covered in this report. It identifies for each area four levels of maturity:

- Reactive: organisations where operational risk losses are seen as a cost of doing business, with little focus on effective risk management
- Compliant: organisations which focus on meeting rules and regulatory requirements
- Proactive: organisations where all staff own risk and take responsibility for improving its management
- High reliability: organisations where risk management is fully integrated into continuous improvement systems Staff at all levels take full ownership of risk and feel free to challenge. The company learns from its own and external loss events and actively targets year-on-year reductions in operational risk losses.

This diagnostic, on the following page, is designed to allow companies to benchmark themselves against the industry and to identify the key steps they need to take to become more mature.

The maturity diagnostic, although designed for the insurance industry, has broad applicability across all industries and sectors.

In the next section - Conclusions - we examine some of the key steps companies need to take to transition from one level of maturity to another.

Open collaboration between organisations

Each year, an oil and gas company shares events with industry body the International Oil and Gas Producers (OGP) association. All OGP members meet for three days each year to review industry trends and the results of major event investigations, in order to reach an agreement as to how the industry can work to address the issues identified.

This approach in the energy sector can be compared to ORIC which focuses on the exchange of anonymised data and best practice.

Maturity Diagnostic

	Reactive	Compliant	Proactive	High reliability
Open environment for reporting	• Only significant loss events are reported • Lack of leadership involvement • Inconsistent reporting processes • Fear of blame/reprimand impedes reporting • People are unsure what to report and why • Reporting delegated to the 2nd line • Near misses not reported	• Coherent process for people to report loss events • Most events reported • Key people are risk aware • Key people understand how to report a risk event • Little focus on near miss reporting	• Everyone feels encouraged to report risk events • Simple standardised company-wide approach to reporting • Ownership of reporting at 1st line • Selected staff at 1st line of defence staff are focused on risk • Staff understand the need to report near misses. >50% are reported	• Single, simple approach to capture enterprise-wide risks • Everyone understands the current and potential risks they face • Everyone understands the need to report risk events and do so directly • Open, learning culture sees events as an opportunity to improve • Near misses actively reported in order to reduce frequency of loss events
Risk event analysis, investigation and impact assessment	• Focus on addressing recovery from loss events • Leadership seek to identify responsibility and blame • Root cause analysis (RCA) not conducted	• Root Cause Analysis (RCA) conducted for priority events • Focus on controls, processes and systems – not behaviours • Ad hoc and inconsistent approach to RCA - few standard tools • Little trained investigative capability	• Clear thresholds for Root Cause Analysis (RCA) • Standard, proven tools and approaches used to conduct RCA • Behavioural root causes always sought • Strong trained capability to conduct RCA • Top leadership reviews causes of major events	• Deep Root Cause Analysis (RCA) for key loss events and major near misses • Analysis identifies trends and causes from high volume minor events • All leaders are seen to engage in RCA • Focus on behaviours (why people acted that way) • Leadership, behavioural and cultural issues confronted • Quality assurance of investigations through peer and 3rd line review
Action management	• Actions for most loss events are not monitored or followed up • Follow-up for major events is on ad hoc basis	• Actions often derived so that they can be delivered rather than make a difference • Actions are managed, monitored and closed • Approach and tools for action management are not consistent across company	• Actions derived to make a difference • Actions are prioritised based on resources available and risk appetite • Actions clearly tracked and only closed on evidence • Top leadership review actions for major events	• Action management process integrated into company-wide continuous improvement approach • Actions may involve replacing existing controls that are not cost effective, not just adding additional controls
Learning and continuous improvement	• No systematic approach in place to learn from internal or external risk events • Learnings tend to be ad hoc and rely often on informal networks	• Changes to policies and procedures occur in response to significant internal risk events • Learnings not always shared across all relevant parts of the company • Review of major external loss events is not systematic	• Processes in place to prioritise and share learnings across the company from internal risk events • Learnings are derived from external risk events • Appropriate ORIC data shared with 1st line • Multiple channels used to engage staff in learnings • The 3rd line review learning effectiveness	• Learnings from loss events and near misses used to deliver year on year reductions in risk exposure • Rigorous approach optimise behaviours and controls based on learning from internal and external events • Proactive sharing and learning across the industry to reduce sector-wide operational and reputational risks

CONCLUSIONS

Currently, there are a wide range of operational risk management practices across the insurance industry. Even companies of similar scale and in the same area of business show markedly different levels of maturity around their approach to risk management.

Our research suggests that there is a significant prize for the industry to reduce the levels of operational risk related to both financial and non-financial losses.

We have observed that organisations with strong risk management approaches systemically address leadership, staff capability and awareness, governance, and robust processes and systems.

Maturity Diagnostic

There is a real opportunity to reduce the cost of operational risk across the industry by applying the maturity diagnostic on the previous page, which identifies four levels of maturity:

- Reactive: organisations where operational risk losses are seen as a cost of doing business, with little focus on effective risk management
- Compliant: organisations which focus on meeting rules and regulatory requirements
- Proactive: organisations where all staff own risk and take responsibility for improving its management
- High reliability: organisations where risk management is fully integrated into continuous improvement systems. Staff at all levels take full ownership of risk and feel free to challenge. The company learns from its own and external loss events and actively targets year on year reductions in operational risk losses.

Moving from ‘reactive’

We have identified three key levers for organisations which wish to improve from a reactive approach:

- Build a compelling benefits case: covering both financial and non-financial benefits
- Gain leadership support: create strong, visible, executive level sponsorship
- Increase awareness and knowledge: of operational risks, reporting processes, and the benefits of reporting, through a major engagement programme.

As leaders and staff focus on understanding the operational risks they face and the benefits of risk event reporting, organisations will quickly strengthen their operational risk management. Typically, organisations can expect to see a temporary increase in loss events as reporting improves.

Organisations should be wary of creating a systems and process based solution, although this may meet regulatory requirements. Without effective leadership and staff engagement, such systems-led transformations are notorious for not producing real benefits and for being unsustainable. Successful organisations have initially built simple tools and templates (such as electronic forms) rather than depending on off-the-shelf systems. Improvements to these basic tools can be made quickly and adapted to business requirements. In all but the smallest organisations, this information will then be captured on the corporate risk system.

Moving towards ‘proactive’ and ‘high reliability’

Best practice in other sectors identifies four key areas:

Near miss reporting

A focus on reducing the incidence of near misses will reduce the number of loss events. Other sectors have demonstrated that addressing near misses will quickly deliver tangible results. Some insurance organisations reported that they treat small loss events as large near misses, but others report difficulties in achieving accurate near miss reporting.

Behaviours and culture

Best practice in other industries is to give the same weight to addressing behavioural failures as is given to system, control and process failures. Only by focusing on behaviours can organisations become mature. There was almost universal recognition from the insurance companies interviewed that behavioural issues lie at the heart of most loss events. Many report a developing focus on addressing culture.

Root cause analysis tools for analysis and investigations

Other industries use proven industry-wide approaches and tools, resulting in robust and consistent analysis and investigations which give management full confidence. This also facilitates the sharing of lessons across the sector. Most of these tools are suitable for use when investigating risk events and we have recommended three for adoption: Five Whys; Fishbone/Ishakawa; and Bowtie. Many of the organisations interviewed recognise that moving from a relatively ad hoc approach to investigations to a more systematic approach centred on proven tools is a quick win.

Become a learning organisation

World class operational risk managers supplement data from their risk event reporting process with data from other areas of the organisation and external risk events. There is an opportunity for many insurance companies to use more data from ORIC reporting across the sector to supplement internal learnings. Using external data helps businesses to create a culture of ‘vulnerability and challenge’ where all staff are actively conscious of potential risk events that may occur and proactively strengthen operational risk controls. In addition, best practice organisations use their learning actively to target year-on-year reductions in operational risk losses.

APPENDIX 1
Tool: Five whys

Example problem: The policy was mis-priced

1. Why?

   A: The pricing system produced the wrong number.

2. Why?

   A: The data used by the system was incorrect.

3. Why?

   A: The pricing model producing the data contained a calculation error.

4. Why?

   A: The pricing model was not quality checked after it was developed three years ago.

5. Why? (a root cause)

   A: No policy is in place to ensure pricing tools are audited after pricing updates.

6. Why? (optional)

   A: Each pricing model is manually built and developed differently, making creation of a single policy challenging.

- **Solution to fifth 'Why?'** Start auditing the pricing model after each pricing update prior to going live
- **Solution to sixth 'Why?'** Automate pricing models to ensure consistency and standardisation.

Objective and when to use it

Five Whys is a simple iterative question-asking technique used to explore the cause-and-effect relationships underlying a problem. The primary goal of the technique is to determine the root cause.

The 'five' derives from an empirical observation on the number of iterations typically required to resolve the problem - five iterations are not mandatory.

Approach

1. Gather a team of people who are knowledgeable about the relevant processes and the event and define the problem statement, eg. 'The policy was mis-priced'.
2. Ask the first 'why' of the team: Why is this taking place? You will probably end up with three or four plausible answers. Write them on a flip chart or whiteboard, or use index cards taped to the wall. Leave plenty of room around them.
3. Ask four more successive 'whys' - repeating the process for every statement. Post each answer near its 'parent' statement. Follow up on all the answers which seem likely. You will have identified the root cause when asking 'why?' does not yield any more useful information. Continue to ask questions beyond the fifth question if necessary to get to the root cause.
4. Among the answers to the last 'why?' look for systemic causes or sources of the problem. Circulate these among the team for discussion. Try to identify one or two most likely systemic sources of the problem. Follow the team session with a debriefing - show the work product to others and ask if they see the logic in the analysis.
5. After settling upon the most likely root cause of the problem and obtaining confirmation of the logic behind the analysis, you can go to work on development of an appropriate corrective action or mistake proofing to remove the root cause from the system.

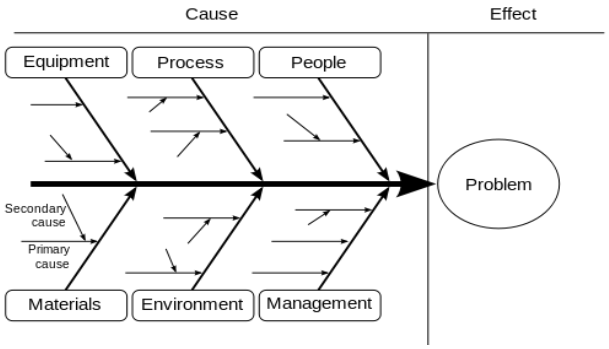
Benefits

- It helps you to quickly determine the root cause of a problem
- It is simple and easy to learn and apply - there is no great training requirement
- It provides input into a fish-bone diagram (below).

Concerns

- Applies to simple, linear issues. In particular, it is not as suited for use with complex events with multiple interlinked causes.

APPENDIX 2
Tool: Ishikawa/Fishbone



Objective and when to use it

The fishbone diagram helps to provide structure to brainstorming sessions determining the causes and root causes of a risk event.

Approach

1. Gather a team of people who are knowledgeable about the relevant processes and the event and define the problem statement.
2. On a whiteboard, draw a line pointing off to the right attached to the problem statement, such as 'incorrect pricing of a policy'. This is the 'effect' part of the cause and effect diagram.
3. From this main line, create branches for various cause categories. These can either be placed first, to fuel brainstorming, or deduced as you go through the process, refining as you continue discussion.
4. Review the major root causes of the event and prioritise which are the most important.
5. Agree the relevant actions to be taken in order to address the root causes.

Benefits

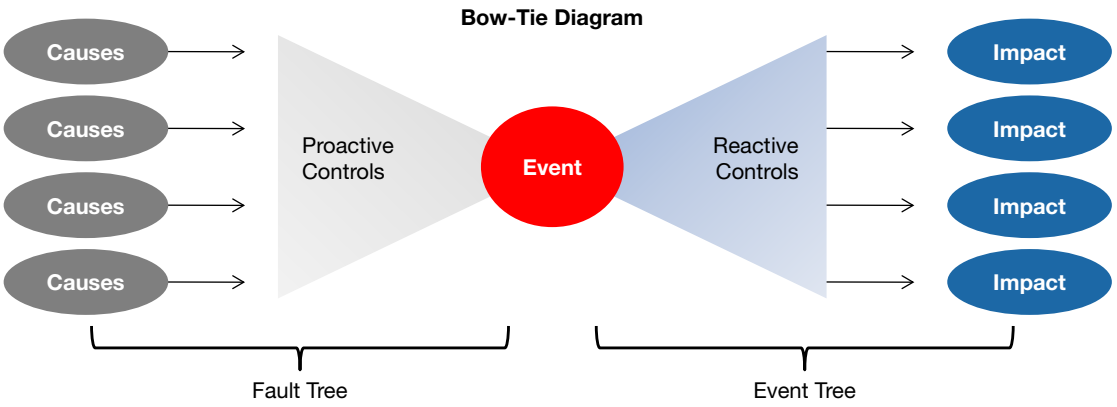
- It is a simple and comprehensive visual tool which can be used to facilitate a team discussion to analyse all but the most significant and complex risk events
- It is easy to use, and does not bring a significant training overhead.

Concerns

- Does not factor in the performance of current barriers and controls.

APPENDIX 3
Tool: Bow tie model

Objective and when to use it:



The Bow Tie model is an accessible visual representation of the potential causes of a loss event and the barriers in place to stop such an event occurring. It also represents the potential impacts from the loss event, and the barriers or mitigation steps to reduce these, meaning the entire pre- and post-event data can be summarised. This enables leadership, risk professionals and front line staff to effectively engage in scenario planning, investigation and learning.

The model can be used online or on paper, with the former application facilitating drill-down interrogation of as many levels as is appropriate. It is a well-proven tool used extensively, including being an industry norm in the in asset intensive and the security sectors.

It can also be a powerful tool to assess the cost-effectiveness of controls to optimise the use of resources and potentially to identify less effective controls that can be modified or removed.

Approach

1. Gather a team of people who are knowledgeable about the relevant processes and the event and define the problem statement, eg. 'The policy was mis-priced'. Place this risk event in the centre of the 'bow tie'.
2. For each major risk event, brainstorm, analyse and group the following:
   - Potential causes or threats - potential root causes of the risk event, eg. no audits of pricing model
   - Potential outcomes or impacts - potential effects of the risk event, eg. over-payment and regulatory fine
   - Barriers (proactive/reactive) - what barriers can be put in place or are in place to prevent the risk event occurring, eg. automating the pricing model; or what barriers can be put in place to minimise the outcome if the risk event has already occurred, eg. immediate communication to impacted customers and closure of new policies being written using the model. The cost-effectiveness of these barriers can be quantified.
3. Review the themes identified, review how the risk is managed today, and identify gaps.
4. Develop actions to close out gaps and agree ownership.

Benefits

- It is a well-proven holistic tool, providing a comprehensive picture of the risk and controls in place
- It is a visual analysis and communication tool which can be shared by leadership teams, risk professionals and frontline staff, and can powerfully engage and educate
- It can be used proactively as well as reactively
- It builds on the fishbone diagram methodology
- It can be expanded to provide quantitative analysis, eg. on the cost-effectiveness of different barriers.

Concerns

- Can be resource intensive, so is more suitable for use in planning to mitigate, or in investigation of, top risk events.

ORIC Members

Admin RE	Andy Huntley
AEGON UK	Robert Galway, Ronnie Scott
Allianz Insurance	John Joyce; Stella Clarke; Imran Shah
AMLIN	Alex Hindson, Neil Trantum, Kirsty Drinkwater
Aviva	Angus Eaton, Adam Stanley
AXA	Layla Peirce
Catlin	Kay Haggis, Gladys Cheung
AIG	Mitesh Shah, Tara Miran
Delta Lloyd	Erik Van Der Zouwen, Gijsbert Hendriksen
Direct Line Group	Ellie King
Ecclesiastical Insurance	Flavia Jones, Simon Arundel
Friends Provident	John Clarke, Lianne Frost
HSBC Life (UK)	Jason Rose, Jim Farmer
Hiscox	David Oliver, James Beach
Insurance Australia Group	Paul Tito
Just Retirement	Elspeth Hyde, Craig Stapley
Legal & General Insurance	Greg Clark
Liverpool Victoria Insurance	Nigel Shrewsbury, Kevin Tidman
Pension Insurance Corporation	David Godfrey, Paul Morrish
Phoenix Group	Andy White, Tracey Reedman
QBE Europe	Kerry Row
Royal Sun Alliance	Surjit Johal, Sandy Craddock
Royal London Group	Steve McIntyre, Melanie Merritt
Lloyds Banking Group	Gillian Sawyers, Katie Taylor
Suncorp	Barry Poole
Travelers	Mark White, Stephen Yates
Wesleyan	Lexine Sentence, Ross Easterby

Research team

ORIC	Caroline Coombe, John Joyce, Imran Shah
Oliver Wyman	Vikram Jain, Crispin Ellison, Kate Wildman
Copywriter	Rowan Morrison

—ORIC

ORIC (Operational Risk Consortium Ltd) is the leading operational risk consortium for the (re)insurance and asset management sector globally.

Founded in 2005 to advance operational risk management and measurement, ORIC facilitates the anonymised and confidential exchange of operational risk data between member firms, providing a diverse, high quality pool of qualitative and quantitative information on relevant operational risk exposures.

As well as providing operational risk data, ORIC provides industry benchmarks, undertakes leading edge research, sets trusted standards for operational risk and provides a forum for members to exchange ideas and best practice.

ORIC has over 30 members with accelerating growth.

www.abioric.com/home.aspx

—About Oliver Wyman

Oliver Wyman is a global leader in management consulting. With offices in 50+ cities across 25 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm's 3,000 professionals help clients optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities. Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC], a global team of professional services companies offering clients advice and solutions in the areas of risk, strategy, and human capital. With over 53,000 employees worldwide and annual revenue exceeding $11 billion, Marsh & McLennan Companies is also the parent company of Marsh, a global leader in insurance broking and risk management; Guy Carpenter, a global leader in providing risk and reinsurance intermediary services; and Mercer, a global leader in talent, health, retirement, and investment consulting.

For more information, visit www.oliverwyman.com.
Follow Oliver Wyman on Twitter @ OliverWyman.