Institute of Risk Management

Fuelling the debate

Latest risk management trends in the energy sector 2019

irm

Developing risk professionals

"IRM qualifications have proved very critical in defining my career as a risk professional. They have been practical in developing an implementation of ERM frameworks and our organisation has become a pace setter in the sector."

Samuel Kibaara, CFIRM
Director, Risk Management Consulting
Pinebridge Training and Consultants Ltd

"IRM qualifications are an excellent way to ensure that you stay relevant and on top of the ever so changing risk management field. It has taught me so many things especially in the areas where I do not see myself as an expert."

Carla Knight IRMCert
Risk Management Specialist
Exxaro, South Africa

"The IRM provided me with the most efficient and robust method of getting qualified to have recognised my standard of knowledge in risk management. Achieving certification was also to be my catalyst for pushing forward in the risk management field, developing myself and others further."

Mike Stark, CMIRM
CRO, Peninsula Petroleum

Executive summary

The energy sector is undergoing rapid change. Following several years of belt tightening and cost cutting, many oil and gas companies are looking to expand into new projects and territories, and into renewable energy sources, according to IRM's energy survey 2019.

Cost cutting and safety naturally remain key areas of focus. But the survey found that businesses plan to invest in new projects because they are confident of achieving profits despite a long period of low oil prices.

Strategic risks, the global economy and an evident skills gap are considered top risks. Only 27 per cent of respondents rated green energy as an area of concern over the next five years, raising the question whether the sector has fully digested the regulatory changes that will, for example, see electric cars as the norm in Europe after 2035.

Risk managers are preparing to respond to this change of emphasis. What is perhaps striking is the wide range of risks they are concerned with across their enterprises. Project management risk, operational risk, technical safety and enterprise risk management (ERM) top the list of areas that will get more attention in the coming months. Business continuity, security and supply chains are not far behind.

The survey also assessed the level of risk maturity across the industry. The results are a little dispiriting, as the sector scored only three out of five. Domenic Antonucci describes this as "... disappointing for a sector with the history, sophistication, management talent and resources of oil and gas," in *Moving up the risk maturity curve for the oil and gas sector* (pages 37-41).

Some risk managers described as problematic a lack of resources and a failure of the board to provide the right tone at the top. Only about 40 per cent of respondents, for example, said they had specialist ERM software, something that whilst not essential, you would expect from major energy companies for properly implementing risk management across large, geographically dispersed organisations.

In light of these findings, IRM wanted to provide insights and thought leadership to risk managers in the sector. In addition to an exploration of the survey results, we have therefore asked industry-leading specialists to provide their advice on how risk managers can improve their performance and relevance across a range of topics – from safety and sustainability to improving risk maturity and building effective risk cultures. These are mentioned in the survey results and contained in two *Insights* sections after each of the main parts of the survey.

About the IRM

The IRM is the leading professional body for Enterprise Risk Management (ERM). We drive excellence in managing risk to ensure organisations are ready for the opportunities and threats of the future. We do this by providing internationally recognised qualifications and training, publishing research and guidance, and setting professional standards.

For over 30 years our qualifications have been the global choice of qualification for risk professionals and their employers. We are a not-for-profit body, with members working in all industries, in all risk disciplines and in all sectors around the world.

This year the IRM will place significant emphasis on supporting businesses and risk professionals on how to understand, manage and take advantage of game-changing risks such as cyber. The recent launch of our new Digital Risk Management Certificate, which was developed with support from Warwick University, is part of this initiative.

Through the IRM's qualifications, training and thought leadership, including the launch of the Cambridge Judge Business School and IRM research report, *Risk Management Perspectives of Global Corporations,* which highlights the top global risk management concerns over the next 12 months. The Institute encourages leaders to think tactically and strategically about change and to question whether and how a threat can be turned into an opportunity. Risk professionals will be key strategic advisers in this journey.

Foreword

Socrates Coudounaris, BEng (Hons) MSc FCII CIP CFIRM

IRM Chair

Risk Management Director, RGA International Reinsurance Company

As the global professional body for the risk management sector, the Institute of Risk Management is delighted to publish this document from our member experts in the energy sector.

We are also pleased to have the opportunity to launch the document at the prestigious Kuwait ERM conference taking place in January 2019. Our relationships with firms in the region have always been excellent and we welcome the opportunity to strengthen them further.

Excellence in risk management requires a strong understanding of general concepts and techniques but also an appreciation of the detailed risk landscape in particular sectors. IRM encourages its members to form sector networks to share knowledge and to work together to develop new thinking and insights.

Our recent work with Cambridge University took a high level cross sector view of the risk management perspectives of global corporates. This specialised study from our energy specialists complements the Cambridge work with a more sharply focused look at the practical application of risk management in the energy sector.

We intend to build further on these initiatives and conduct more specialist academic research with Cambridge during 2019. We also intend to develop an ongoing special interest group for the energy sector that will support risk professionals in the field.

It is particularly interesting to note that one of the conclusions of this document is that there is great scope for raising levels of risk maturity in this globally important sector. This will require attention to various aspects of risk management and particularly to competence, training and education, raising them to world class standards. The IRM stands ready to play its part in this process.

I would like to thank all the individuals who contributed to this work and completed the survey. In particular, thanks are due to IRM Certified Fellow Alexander Larsen who led and co-ordinated the project.

Contents

Survey Results part I: Energy industry in change

The largest risks facing the energy sector are strategic in nature, according to most respondents (see *Where do your biggest risks come from?*) This is not surprising from an ERM perspective since strategic risks are difficult to insure and can have a major impact on a company's performance and – increasingly – its reputation. Operational risks scored highly, followed by financial and people-related risks.

While these results may have been predictable, the nature of the risk landscape is changing – both affecting how companies are altering the focus on their businesses and the way they manage risk.

The biggest story in the energy sector over the past few years has been the collapse of the price of oil.

Where do your biggest risks come from? (1 low and 5 high)

	1	2	3	4	5
Strategic	2.94% 1	5.8% 2	11.76% 4	17.65% 6	61.76% 21
Operations	0.00% 0	0.00% 0	17.65% 6	41.18% 14	41.18% 14
Financial	0.00% 0	3.03% 1	33.33% 11	45.45% 15	18.18% 6
Compliance	6.06% 2	30.30% 10	30.30% 10	15.15% 5	18.18% 6
IT	3.03% 1	15.15% 5	36.36% 12	33.33% 11	12.12% 4
People	5.88% 2	5.88% 2	32.35% 11	29.41% 10	26.47% 9
Geographical	5.88% 2	23.53% 8	47.06% 16	5.88% 2	17.65% 6

When asked *How important do you think the following risks are to your organisation in the next two to five years?* About three in four respondents ranked it highly.

More recently, regulators around the globe have switched their attention to renewables. For example, the European Union has said that by 2035 all new cars sold in the zone will be electric. This is a major shift and puts pressure on oil and gas companies to reconsider their strategic and business models. Not only will they need to consider their target markets and offering carefully, they will need to plan long-term about the very nature of their businesses. It is, perhaps, surprising that only 27 per cent of respondents to the survey ranked green energy issues significant or major in the next five years, raising the question over whether they are rising to the challenge. The nature of the global economy (77 per cent) and the growing skills gap (50 per cent) feature much more prominently.

Most organisations felt that major accidents and incidents were well managed and feature it as a very low risk. That raises a new challenge: how do companies improve safe operations in an industry that already has a lot of controls in place? Iain Wilson, senior principal consultant, DNV GL – Oil & Gas, explores such issues in his article *Maintaining safe operations – is it time for a "verification scheme" for management systems?* (pages 11-14).

Future focus of the energy industry

Despite a few years of heavy job cuts and cost reduction programmes, the survey found that the energy industry is still concentrating on cost reduction and organisational efficiency (see *What will be the main area of focus for your organisation in the coming years?*). More positively, respondents said they were turning their attention to new projects, exploring fresh territories and diversifying into renewable energies.

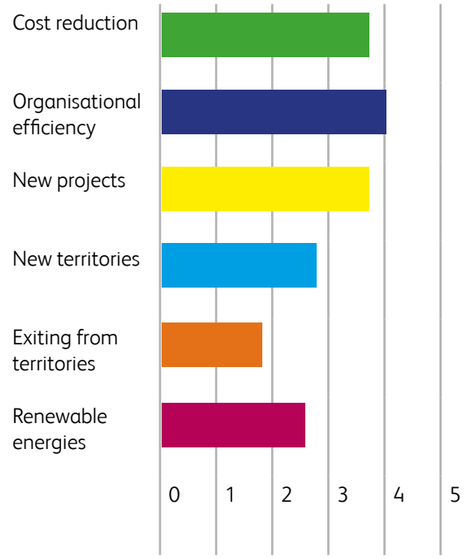
How important do you think the following risks are to your organisation in the next 2-5 years?

(1 - not at all, 2 - somewhat, 3 - significant, 4 - major)

	1	2	3	4
Oil price	3.33% 1	10.00% 3	6.67% 2	80.00% 24
Major accident or incident	46.67% 14	20.00% 6	16.67% 5	16.67% 5
Cyber attack	33.33% 10	46.67% 14	10.00% 3	10.00% 3
Skills gap	13.33% 4	36.67% 11	40.00% 12	10.00% 3
Regional instability	6.67% 2	60.00% 18	30.00% 9	3.33% 1
Regulatory changes	10.00% 3	43.33% 13	36.67% 11	10.00% 3
Supply chain failure	26.67% 8	36.67% 11	26.67% 8	6.67% 2
Failure of new business ventures	33.33% 10	33.33% 10	26.67% 8	6.67% 2
Technological changes	26.67% 8	33.33% 10	33.33% 10	6.67% 2
Green energy focus	40.00% 12	33.33% 7	13.33% 4	10.00% 3
Natural disaster	60.00% 18	23.33% 7	13.33% 4	3.33% 1
Global economy	6.67% 2	16.67% 5	53.33% 16	23.33% 7
Compliance failure	36.67% 11	40.00% 12	20.00% 6	3.33% 1

What will be the main area of focus for your organisation in the coming year?

(1-5, where 5 is a priority focus)



This indicates a period of change for the industry as businesses look to longer-term strategies for growth while improving efficiencies. As Mark Boult of DNV argues in his feature *Gas capital expenditure boost to fuel the energy transition* on pages 13-15, confidence is growing because the past few years of intensive cost cutting has created confidence among businesses that they can now be profitable even though oil prices remain low.

"The big change in industry confidence is not because of a belief that the oil price is going to rise to previous levels," said Graham Bennett, vice president, DNV GL – Oil & Gas, one participant to a DNV survey. "But instead because industry participants now have their cost levels under control and can make a reasonable margin, even at $55 or $65 per barrel of oil."

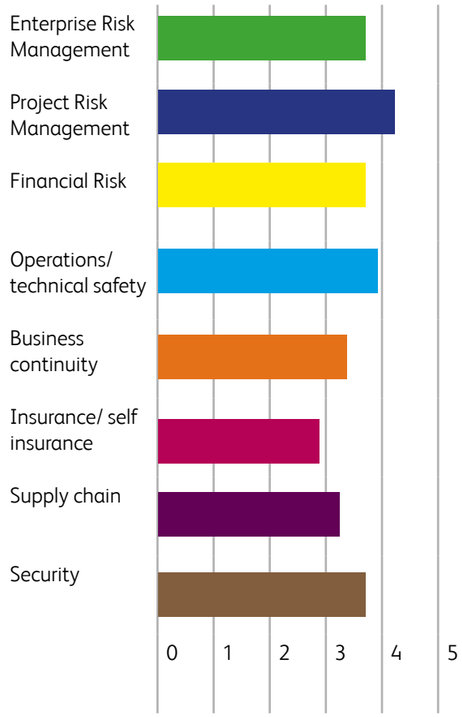
This trend could be positive for risk management, which plays a vital part in ensuring the resilience and continuity of the business, including driving down unforeseen costs. There is fresh impetus to consider integrating ERM and sustainability, Manivannan R Rajan of Comtec Management Consultants argues in *Integrating enterprise risk management and sustainability in the oil and gas industry* (pages 18-22) He argues that "Large corporations now need to take much more responsibility for development than ever before, as they have become dominant institutions on all dimensions of sustainability." The solution he offers is the holistic management of risks from the joint perspectives of enterprise and sustainability. "Such an integrated approach alone can ensure efficient management of risks and uncertainties, besides enabling the organisations in the industry to seize opportunities and help in achieving a successful energy

Future risk management focus

When survey respondents were asked *What will be the main area of focus with regard to risk management within your organisation over the coming years?*, project risk management, ERM and business continuity all scored highly – although operational and technical safety remained a core concern. Balancing these areas will be essential as organisations seek to explore new areas of business while keeping the safety and efficiency of operations optimised.

What will be the main area of focus with regards to risk management within your organisation over the coming years?

(1-5 where 5 is a priority focus)



The wide spread of responses to the categories within this question reflects the range of professional disciplines that play a part in reducing accidents, fraud, fines, exchange rate costs and other similar risks. In these areas ERM and financial risk management can support decision-making in terms of both financial and strategic upsides and downsides, as well as improving contract negotiations.

Key areas of risk management focus that support new projects, territories and renewables were:

1. Business continuity management
2. Project risk management
3. Security
4. Supply chain

These risk management disciplines have a major impact on improving project costs and schedule overruns by effectively managing suppliers, equipment delivery times and costs. In addition, they can help manage disruption as a result of strikes, protests or other security-related risks.

Business continuity management

The survey found that over 40 per cent of organisations have business continuity plans in place (see *Are there business continuity plans?*) with just over 30 per cent indicating that they were "somewhat" in place, suggesting further work needs to be done in order to update them or improve on them. One in five (20 per cent) respondents said they plan to put such plans in place.

Major incidents and accidents are key areas of concern for oil and gas organisations. The Deepwater Horizon incident, for example, caused the loss of 11 lives and injury to 17 others, and led to an oil spill off the Gulf of Mexico which is now considered the largest offshore spill in US history. The disaster highlights the need for good risk management before, during and after such events.

Lisa Khan, in *What is business continuity management?* (pages 23-25), explains how business continuity can be effectively implemented by risk management. In this context, risk management seeks to prevent incidents from occurring, deal with them effectively if they do and provide effective recovery once an incident is over. She says that businesses should follow a good crisis management and contingency plan during an incident. Such plans should be clear, concise and easy to use, and include a media management plan.

Project risk management

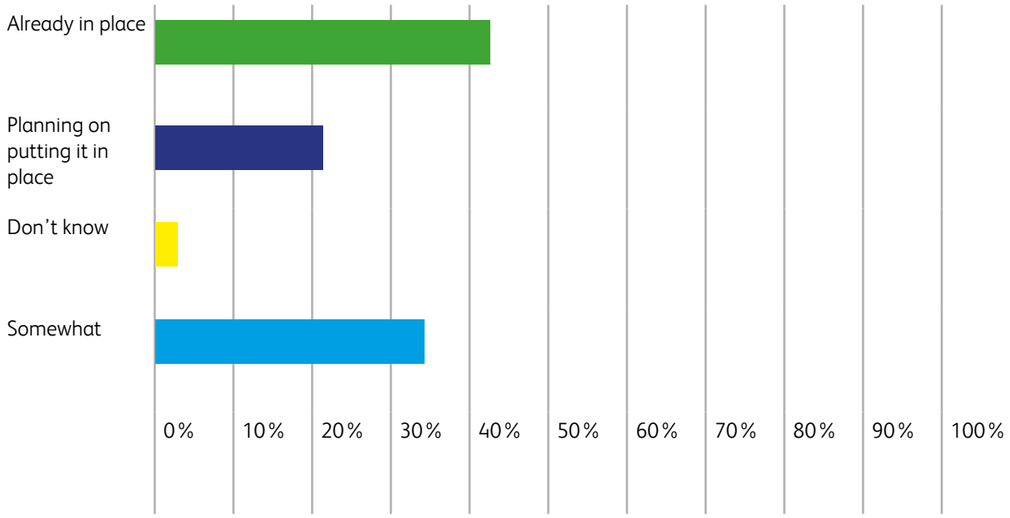
It is no surprise that energy companies are investing time in improving and implementing project risk management given the drive to initiate new ventures. Done correctly, project risk management can help project managers deliver within schedule and under budget and, at the very least, it can contribute to reducing overruns.

Peter Smith, Partner at QuantPro, argues in *The lean start-up – a new approach to implementing portfolio contingency management* (pages 26-30) that risk managers must be able to support companies looking at a portfolio of projects, especially when there are interdependencies, such as when the start dates of projects rely on completion of other initiatives. He outlines in detail his approach to implementing portfolio contingency management.

Supply chains

Robust supply chains are vital to the success of any project, and increasingly supply chain management is becoming crucial to the protection of reputation as well as meeting more stringent regulations and law such as fraud, modern slavery and competition law. Security too is a key concern among energy companies who often are working in sensitive regions.

Are there Business Continuity Plans?



Maintaining safe operations – is it time for a "verification scheme" for management systems?

Iain Wilson

Senior Principal Consultant, DNV GL - Oil and Gas

Betteridge's Law suggests that any newspaper headline that ends with a question mark can be truthfully answered with the word "no". Finding the right answer to the question in the headline may not be quite so straightforward.

It is universally recognised that Process Safety Management (PSM) or the management of Major Accident Hazards (MAH) relies on the interaction between "Plant", "Process" and "People" risk management barriers.

For offshore production installations there exists in law, under the EU directive on Offshore Safety, a requirement for the independent verification of the suitability and sufficiency of the arrangements for the inspection, test and maintenance of the "Plant", namely, verification schemes for the management of Safety and Environmentally Critical Elements (SECEs).

It is becoming apparent, from ongoing incident histories, that weaknesses, actual and potential, in the "Process" and "People" aspects of risk management are creating opportunities for major incidents. The findings of the Offshore Safety Directive Regulator's (OSDR's) first round of In Depth Maintaining Safe Operations (ID MSO) audits supports this and highlights the organisation's increased level of attention in this area.

It is estimated that around 40 per cent of ignited process safety incidents occur during normal, steady-state operations, while 60 per cent result from transient activities, such as start-up and maintenance. This needs to be set against the background that transient operations only account for a small fraction of the running time for any particular piece of equipment.

It can be argued that normal operations can be more reliant on "Plant" barriers and that transient operations

are more significantly controlled by “Process” and “People” barriers. If this is accepted, it can then be inferred that these barriers are the “weak links” in the overall risk management picture. As this is clearly not the intended outcome, it suggests that the position of these non-Safety and Environmentally Critical Elements (SECE) barriers is one of “poor relations” in terms of assurance. This may be leading to less dependable performance of these barriers.

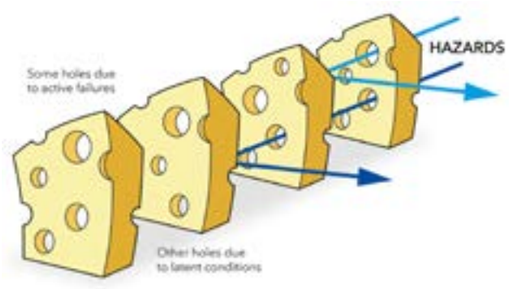
Is it time for the “Process” and “People” barriers to be subject to the same level of independent scrutiny as the SECEs and for verification to be extended to management systems? And, if the verification of “Plant” barriers encompasses the inspection, testing and maintenance of these barriers as well as checking these activities are suitable and sufficient, what are equivalent processes to support the “Process” and “People” barriers?

The sections below examine the approach taken for SECE assurance (“Plant” barriers) and compare it with the approach taken for Safety and Environmental Management Systems (SEMS), encompassing “Process” and “People” barriers. Some specific questions prompted by some of the differences are highlighted.

Identification of critical barriers

SECEs are identified from the formal safety assessment and are broadly defined in the Prevention of Fire and Explosion, and Emergency Response (PFEER) regulations. Identified SECEs across all installations show a high degree of commonality.

Figure 1: Successive layers of defences



Offshore Safety Case Regulations (OSCR) 2015 guidance gives no clear definition or guidance to identify critical SEMS-related barriers. While tools such as bowtie analysis can assist in the identification of critical SEMS elements, these processes most commonly focus on SECEs. SEMS elements are dealt with superficially, if at all. The technique can be applied to identifying the management system elements which are critical to managing MAHs. Additionally, information from incident investigations and audits can provide indications of the criticality, strengths and weaknesses of SEMS elements, if root cause analysis is carried out effectively and the findings are analysed sufficiently.

Performance standards

For each SECE, a performance standard describing the required operation of the SECE is developed. This is commonly expressed as a description of the required functionality (what the SECE is intended or designed to do), availability or reliability (the required level of confidence that, when needed, the SECE will operate as intended) and survivability (the expectation that the SECE will continue to function during a developing major accident scenario).

KPIs rarely reflect the performance of a single SEMS element

Often key performance indicators (KPIs) are used to measure the health of the overall performance of the organisation. These may be “leading” (measuring the inputs into the system) or “lagging” (measuring the outputs from the system), usually in terms of failures. KPIs rarely reflect the performance of a single SEMS element in isolation. Using KPIs as benchmark criteria or a health indicator for specific SEMS element assessments is likely to be problematic and imprecise.

KPIs should be analysed to ensure that they are measuring the right things. Criteria should be set for audit finding categorisation and these should be used as pass/fail indicators for the health of SEMS elements.

Inspection, test and maintenance

SECEs are subject to a programme of preventative maintenance designed to ensure continued satisfaction of the requirements set out in the performance standard. These commonly take the form of tests to ensure that the functionality is as intended and that test and maintenance intervals are such that the availability/reliability meets the criteria set in the performance standard.

Audit is the primary form of assurance for SEMS elements. This can come in a variety of forms. SEMS audits are typically compliance-focused and follow the definition set out by the European Foundation for Quality Management (EFQM) that “an audit is a check against a defined standard to confirm whether people are doing what they are told they should be doing”. This is necessary but can only provide part of the measures required.

Compliance-based audits can provide information about how the actions set out in the SEMS elements are being followed (analogous to the availability/reliability of SECEs) but cannot provide information about the success of the SEMS element in achieving its intended objective (the functionality aspect).

Audit is the primary form of assurance for SEMS elements

Measurement of how rigorously a particular process is being followed does not tell us anything about the effectiveness of the process nor provide opportunities to identify improvements which can be made.

Some form of assessment, as defined by EFQM as “a learning activity investigating why people have chosen to do things the way they do and what other options have been considered”, would provide the opportunity to explore the effectiveness of the SEMS element and look for opportunities for improvement. These are often less frequent, less systematic and less detailed than compliance audits.

Pass/fail criteria should be set for audits, and specific, targeted KPIs (both leading and lagging) should be defined. It is common for organisations to measure and trend backlog relating to SECE maintenance and this should be also be applied to SEMS. If the audit programme has fallen behind, a risk assessment should be carried out to identify any exposures and put additional safeguards in place.

When known degradations or constraints are put on SECEs, the industry typically instigates an operational risk assessment to mitigate any additional major hazard risk that this presents. Identifying critical weaknesses with SEMS should be treated exactly the same as physical control measures, including how we consider the risks associated with management of change, known impairments and deferral of audits.

Continuous improvement

It is an expectation that the data gathered from the SECE inspection, test and maintenance programme be analysed and, if necessary, the performance standards and underlying risk assessment be updated to reflect the findings. There is also an underlying expectation that the overall risk management performance will improve over time and that risk levels will be reduced.

Figure 2: To drive improvement, objective measurement of SEMS element performance is required

Likewise, there is an expectation that SEMS element performance should be improved over time. This cannot be achieved by compliance monitoring alone as that will only maintain the intended, current situation.

To drive improvement, objective measurement of SEMS element performance is required and the processes themselves must be examined for opportunities for improvement.

As described in the HSE *Managing for health and safety* guide, the current favoured management model is “Plan, Do, Check, Act”. This is a departure from the previous policy, organising, planning, measuring, audit and review model. Although audit is no longer a specific management system element, it is noted as being integral in both the check (the audits themselves) and act (learning from the audit findings) phases. Therefore a combination of audit and measurement is required to measure SEMS elements performance to demonstrate improvement.

The audit must go beyond compliance monitoring and into the realm of the “assessment” and must challenge the effectiveness and efficiency of the SEMS element, potentially benchmarking against best practice and/or implementation elsewhere.

Independent oversight

Verification of SECEs is defined as "a system of independent and competent scrutiny of safety-critical elements throughout the lifecycle of an installation, to obtain assurance that satisfactory standards will be achieved and maintained."

The verifier is required to confirm that the identified SECEs and defined performance standards are suitable and sufficient. They are also responsible for checking that the activities required to maintain the operation in line with the performance standards are being carried out.

SEMS elements are typically audited from within any given organisation. Simple compliance audits are often carried out by line management, and higher-level management system audits may be carried out by personnel from other sections or assets. Corporate-level audits may also be carried out on an infrequent basis. External third-party audits will normally be confined to ISO certification or similar. The use of third-party resources to support and coach internal auditors can be a way of increasing the quality of audit findings and the effectiveness of audits.

The requirement of independent oversight of SECEs gives a number of benefits. A clear, minimum level of performance is defined, deviation or drift from published maintenance plans can be identified and challenged, and the independent party can provide an insight into best practice.

Third-party oversight has the potential to bring many advantages. It offers an incentive to ensure that the audit programme remains on track and provides an external quality check on the audit processes and findings as well as facilitating benchmarking.

Independent assurance and continuous improvement across the entire SEMS could be achieved through use of DNV GL's ISRStm protocols; these present best-practice benchmarks for safe and sustainable management.

Summary

It is clear that all barriers are not treated in the same way, nor is the same degree of scrutiny applied to their performance.

Evidence states that "Process" and "People" barriers, primarily relating to elements of the SEMS, are not as effective or reliable as "Plant" barriers, primarily our SECEs. While there may be inherent reasons why SECEs should be more reliable than SEMS elements, there can be no sound justification for not assuring the performance of the SEMS elements to as high a level as is reasonably practicable. These issues raise pertinent questions on how to identify, measure and assess critical SEMS elements.

OSDR through the ID MSO audits are showing an increased level of interest in specific SEMS-related aspects. Regulations, as they stand, enshrine a different level of oversight for physical barriers, but the question remains: should high-performing organisations (or those who aspire to high performance) limit their activities to those required by regulation?

Gas capital expenditure boost to fuel the energy transition

Graham Bennett,

Vice President Business Development, UK & West Africa, Oil & Gas, DNV GL

The world will need less energy from the 2030s onwards, but it will still require a significant amount of oil and gas in the lead-up to mid-century according to DNV GL's 2018 Energy Transition Outlook.

The independent model of the world's energy system forecasts that rapid gains in energy efficiency will lead to a peak in humanity's energy demand in 2035 at a level some 15% higher than in 2017. Global demand for energy is then set to decline, thanks to increasing and rapid electrification of the world energy mix, in addition to slowing of population and world economic growth over the long term.

DNV GL's Outlook forecasts global electricity demand to rise by some 160% by 2050, thereby increasing its share of total final energy demand from 19% in 2017 to 45%. Renewable energy sources will increasingly dominate world electricity generation, primarily driven by solar photovoltaic and wind (Figure 1).

Despite the rise of electricity generation from renewables, oil and gas will still account for a significant 40% of world energy demand in 2050. The Outlook expects natural gas to overtake oil to become the world's largest source of energy in 2026. In a 'golden age' for gas, it will retain this position through to mid-century when it will account for a quarter of the world's energy supply.

Investment on the horizon

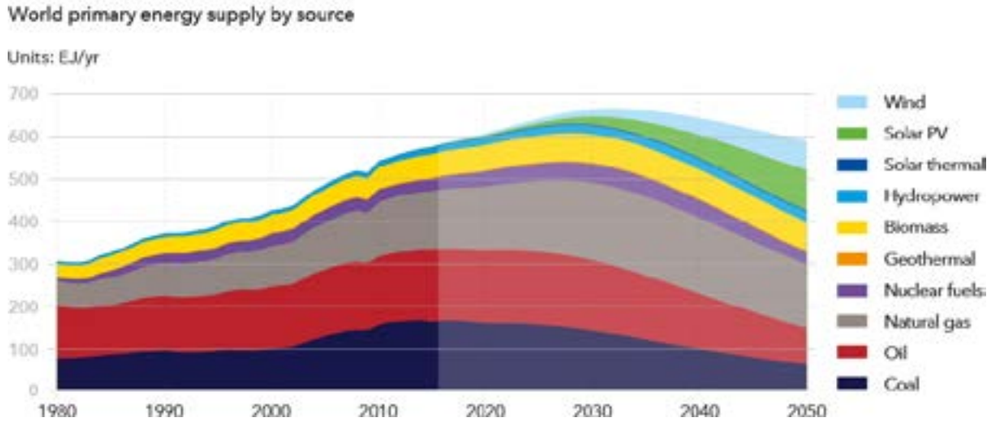
DNV GL's model predicts global oil demand to peak in 2023, while demand for gas, the least carbon-intensive of the fossil fuels, will continue to rise until 2034. New resources will be required long after these dates to continue replacing depleting reserves, and significant levels of investment will be needed to support this shift from an oil-led to a gas-led energy mix.

"Gas will fuel the energy transition in the lead-up to mid-century," said Liv Hovem, CEO, DNV GL - Oil & Gas." It sets a pathway for the increasing uptake of renewable energy, while safeguarding the secure supply of affordable energy that the world will need during the energy transition."

Increasing investment supports gas to fuel the energy transition

DNV GL's Energy Transition Outlook predicts global upstream gas capital expenditure will grow from USD960 billion (bn) in 2015 to a peak of USD1.13 trillion in 2025 to support the transition to the golden age of gas.

Figure 1: DNV GL's 2018 Energy Transition Outlook forecasts that oil and gas will meet 40% of the world's demand for energy in mid-century despite the rise of renewable energy (Graphic: ©2018 DNV GL)



Upstream gas operating expenditure is also set to rise from USD448bn in 2015 to USD582bn in 2035, when operational spending will be at its highest.

This cash injection will enable the 46 % increase in the annual rate of additions to gas production capacity that the Outlook forecasts between 2018 and 2030. Conventional onshore and offshore gas production is forecast to decline from about 2030, while unconventional onshore gas is expected to rise to a peak in 2040.

Among its forecasts for 10 global regions, DNV GL's Outlook sees North East Eurasia (including Russia) and the Middle East and North Africa (MEA) accounting for most onshore conventional gas production in the lead-up to 2050, while North America will continue to dominate unconventional gas production. In the offshore sector, the MEA region sees the highest annual rate of new gas production capacity from now until at least 2050.

Tomorrow's oil and gas industry will not look or behave like it does today, however.

More exploration and production expected

DNV GL's Outlook forecasts new oil fields will be needed until at least the 2040s, while new gas developments will be required beyond mid-century. Production will likely come from smaller reservoirs instead of vast fields, however.

"Most easy-to-produce, 'elephant' fields have been found and are in production.

The remainder that we know about tend to be in Arctic and ultra-deepwater environments," said Graham Bennett, vice president, DNV GL - Oil & Gas. "As oil and gas demand declines, it is unlikely that reserves in such sensitive regions will be developed, due to their high breakeven costs and social impact."

Instead, new resources may be increasingly developed from a greater number of smaller more technically-challenging reservoirs, where leaner, more agile approaches to production will be required, he suggested: "These are more economically viable for emerging, smaller operators looking to develop fields close to existing infrastructure."

To maximize these opportunities in the energy transition, the oil and gas industry needs to continue and step up efforts to become faster, leaner and cleaner, he added.

"Greater use of enhanced, digitally-enabled technologies will be needed to boost production from these smaller reservoirs. It is time for our sector to enhance its focus on developing the digital technologies that will enable quicker and more agile exploration and production."

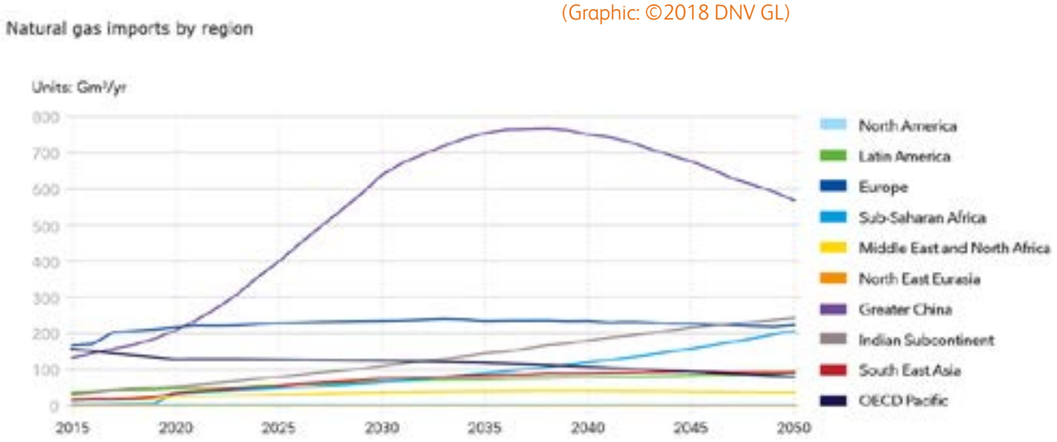
Investing in lower-carbon gas transmission and distribution

Rising global demand for gas will impact activity across the oil and gas value chain, according to DNV GL's Energy Transition Outlook.

The forecasted investment in upstream gas will support the doubling of liquefied natural gas (LNG) capacity that the Outlook predicts between 2018 and the late 2040s. This growth will reflect the industry connecting new sources of gas supply with changing centres of demand (Figure 2).

Figure 2: DNV GL's Energy Transition Outlook model predicts strongly increased gas demand in countries that have less well-established gas infrastructure, such as China and India. This leads to a need for imports in these regions as shown in the graph, alongside the creation of a substantial internal gas infrastructure.

(Graphic: ©2018 DNV GL)



Seaborne gas trade is forecast to treble from North America to China by 2050. An increase in trade from Sub-Saharan Africa to India and South East Asia is also expected.

"We also see the nature of gas beginning to change dramatically, as greener gases – including biogas, hydrogen and syngas – enter gas transmission and distribution networks," Bennett said.

The industry's digital transformation will play a significant role in achieving this, he added. "Data analytics will facilitate more sophisticated midstream and downstream network models to ensure consistent gas quality using mixed gas sources."

Energy Transition Outlook guides strategy and policies for the transition

Despite DNV GL's predictions for a rapid decarbonization of the world energy system, the Energy Transition Outlook forecasts that global warming will likely reach 2.6 degrees Celsius (°C) above pre-industrial levels in 2050. This is well above the 2°C target set out by the COP 21 Paris Agreement on climate change.

"I see it as our sector's responsibility to maintain sharp focus on decarbonization," said Hovem. "For example, DNV GL is supporting operators to validate the technical feasibility of hydrogen-powered gas networks. It will help our sector take a big step forward in significantly reducing its carbon footprint.

She pointed out that the increased uptake of carbon capture and storage (CCS) will also play a role: "The economics of large-scale CCS will improve for energy-intensive activities such as gas-fuelled power generation. But our Energy Transition Outlook model currently forecasts that CCS will capture only 1.5 % of emissions related to energy and industrial processes in 2050. At DNV GL we have a role to play in supporting the policy changes that will be needed to support the large-scale roll-out of CCS in our industry."

The company's suite of 2018 Energy Transition Outlook reports can assist strategy and policy makers to maximize opportunities and minimize risks as the world energy system evolves. The main Outlook report covers the transition of the entire energy mix to 2050. It is accompanied by three supplements forecasting implications for the oil and gas, power supply, and maritime industries. All are available free of charge.

Download the 2018 Energy Transition Outlook reports from: **eto.dnvgl.com**

Integrating enterprise risk management and sustainability in the oil and gas industry

Manivannan R Rajan CFIRM

Comtec Management Consultants

These are truly exciting and challenging times. Huge economic developments and technological advancements co-exist with equally troubling issues and problems.

Pundits rate technology, globalisation and climate change as the three largest accelerating forces of the 21st century. Automation, artificial intelligence (AI), the Internet of Things (IoT) and robotics are transforming the way resources are produced and consumed.

On the flip side, the bewildering array of changes in all walks of life have spawned newer risks and challenges.

Growing economic uncertainty, geopolitical instability, regulatory environment, rapid advances in technology, business disruptions, increased volatility of exchange rates and commodity prices, corruption and terrorism are some of the larger factors contributing to a more challenging economic environment.

Contemporary social challenges include population growth, sharp inequalities due to disparities in income and wealth distribution, human rights violations, xenophobia, alarmingly large levels of unemployment, forced migration of people and increase in spread of diseases.

Environmental concerns, at the top of global risks in any study, include climate change and global warming, extreme weather events, loss of biodiversity, chemical pollution, changing land use patterns, desertification and ocean acidification.

We are living in an "era of unprecedented challenges", and compulsorily need to "embrace complexity" to be able to find *sustainable solutions* to save the planet and humanity, according to Jeffrey Sachs in *The age of sustainable development.*

Business organisations are perceived as the drivers of economic progress. They have a major role in effectively managing all the enterprise risks in the economic, social and environmental spheres, in order to meet their strategic objectives and stakeholder expectations.

ERM is the process by which organisations identify, measure, manage and report on all key risks. It is intended to help organisations achieve their strategic objectives, increase value to stakeholders, minimise surprises and losses, and capitalise on opportunities. Sustainability endeavours to balance economic growth with environmental preservation and social inclusiveness.

The subjects of risk management, sustainability and the oil and gas industry are too vast to be covered in a single paper. The objective of the article is to highlight the key aspects covering the domains and the imperatives for their integration and adoption of a holistic approach.

Imperative of ERM

Risk management is "the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities," according to the Institute of Risk Management's professional standards.

The Global Risks Report 2018 of the World Economic Forum has identified 30 risks, spanning five domains: Economic, Environmental, Geopolitical, Societal and Technological. It is apparent that a clear need exists for a robust risk management framework to effectively manage the diverse risks.

ERM enables management to effectively deal with uncertainty and associated risk and opportunity, enhancing the capacity to build value.

A brief overview of sustainability

"Sustainability" has evolved to include environmental, social inclusion and governance dimensions, and is fast becoming an overarching framework embracing all aspects of human existence. The three dimensions – social, economic and environmental – are widely referred to as the "triple bottom line" of business.

Several factors on a global scale, such as globalisation, environmental degradation, population growth, resource depletion, consumerism, social inequality and technological explosion, have contributed to the rise of the notion of sustainability. The world's population is presently at 7.2 billion people, up by ten times since the Industrial Revolution, according to Sachs, with an annual GDP of about $90 trillion (Leadership Council of the SDSN, 2014), up from a base of 5.33 trillion Geary–Khamis dollars (equivalent to $) in 1950.

The Earth is definitely not in a position to handle the double-whammy of a growing population and increased economic activity leading to the disastrous state of our natural environment.

The "Paris Agreement" (2015) saw 196 countries joining together in a universal pact to set the world on the path to a truly global solution towards a zero-carbon, resilient, prosperous and fair future.

On growing inequalities in society, Oxfam's report *Reward work, not wealth* (2018) laments that 82 per cent of the wealth generated in 2017 went to the richest 1 per cent of the global population, while the 3.7 billion people constituting the poorest half of the world saw no increase in their wealth. Credit Suisse (*Global Wealth Report,* 2016) points out that "while the bottom half (of world population) collectively owns less than 1% of total wealth, the wealthiest top 10% own 89% of all global assets".

Confronted with such challenges on multiple fronts, several experts have observed that the current global economic model is the root cause of many of the present-day ills and therefore unsustainable.

Sustainable development gained wide currency with the publication of the Brundtland Commission Report (Our common future, 1987), defining sustainability as "Development that meets the needs of the present without compromising the ability of future generations to meet their own needs".

Sustainability is expected to address many of the shortcomings of the current economic, political and business systems and provide for a more holistic, balanced and integrated approach.

The role of business organisations in managing sustainability

Business organisations are big economic entities and have footprints in all domains. A study in 2016 by Global Justice Now found that: (a) of the world's top 100 global economic entities, 69 are corporations; (b) Walmart, Apple and Shell are richer than Russia, Belgium and Sweden; and (c) the world's top ten corporations have a combined revenue of more than the 180 "poorest" countries. In 2016, the world's 500 largest companies generated $27.7 trillion in revenues and $1.5 trillion in profits (Fortune Global 500 Rankings, 2017).

Business organisations are today facing a new risk reality, as they are increasingly being held accountable for global climate change, fraud, corruption, pollution, labour abuse and more. For failing to act responsibly, a company will be punished in the public opinion, and the environment and society will suffer along with the company's brand reputation.

Large corporations now need to take much more responsibility for development than ever before, as they have become dominant institutions on all dimensions of sustainability.

The major benefits of managing sustainability are improved brand image, greater pricing power, cost savings, employee engagement, innovation, new sources of revenue, effective risk management and enhanced stakeholder relations.

The Business & Sustainable Development Commission (*Better business, better world,* 2017) emphasised the "need to strike out in new directions to embrace more sustainable and inclusive economic models", and pointed out that companies could gain at least $12 trillion by developing sustainable business models.

As sustainability is essentially long-term, it is imperative that business risks are fully integrated with sustainability risks (extending beyond economic risks to the spheres of environment and social risks), to ensure holistic performance.

Oil and gas industry: risks and sustainability challenges

Oil and gas companies are behemoths, with huge economic impacts. China National Petroleum, Royal Dutch Shell, Exxon Mobil and BP figure in the top ten of Fortune's 2017 Global 500 rankings. The top ten have huge assets ($2,929 billion) and revenues ($1,650 billion) (S&P Platts Top 250 Global Energy Company Rankings, 2017).

Assets

Assets rank	Company name	Assets (millions)	Overall Top 250 rank
1	Royal Dutch Shell plc	411275	23
2	PetroChina Co Ltd	352682	57
3	Exxon Mobil Corp	330314	9
4	Electricté de France SA	316984	25
5	RJSC Gazprom	296840	1
6	BP plc	263316	99
7	Chevron Corp	260079	121
8	Petróleo Brasileiro SA	245912	141
9	TOTAL SA	230978	10
10	China Petroleum & Chemical Corp	220530	5

Revenues

Revenues rank	Company name	Revenues (millions)	Overall Top 250 rank
1	China Petroleum & Chemical Corp	284148	5
2	PetroChina Co Ltd	237937	57
3	Royal Dutch Shell plc	233591	23
4	Exxon Mobil Corp	197518	9
5	BP plc	182648	99
6	TOTAL SA	127925	10
7	RJSC Gazprom	107217	1
8	Chevron Corp	103310	121
9	RJSC LUKOIL	91708	6
210	RJSC Rosneft Oil Co	83601	22

The energy landscape is constantly changing with several technical and geopolitical forces at work: the growing share of renewables in the energy mix, the rise of shale and the growing exports of LNG and oil from the US, and Asian refiners looking beyond the Middle East to diversify their sourcing of crude (S&P Platts, 2017).

Factors such as volatility in energy prices, clamour for clean energy initiatives; the shift towards gas; digitalisation; evolving mobility solutions; cost pressures; changing modes of power generation and distribution; and national, state-level and international regulations such as the Paris climate accord are expected to exert huge pressure on the industry and may cause disruptions.

The oil and gas industry (OGI) is associated with major environment hazards, according to the World Bank Group, which include: (a) pollution at all stages of oil and gas lifecycle, wastewaters, gas emissions, noise generation, spills, solid waste and aerosols generated during operations and transportation; (b) intensification of the greenhouse effect, acid rain, poorer water quality and groundwater contamination; (c) biodiversity loss; and (d) energy efficiency and resource conservation, losses due to venting and flaring.

Environmental incidents in the OGI, with huge impacts, are too well known. These include Exxon Valdez 40,000 MT crude oil spill in the Prince William Bay, Alaska, in 1989 and BP's 2010 explosion of Deepwater Horizon in the US.

Similarly, on the safety front, incidents such as the massive explosion at the BP Texas City refinery, and the Buncefield Oil Depot disaster in the UK in 2005, have revealed the soft underbelly of the industry.

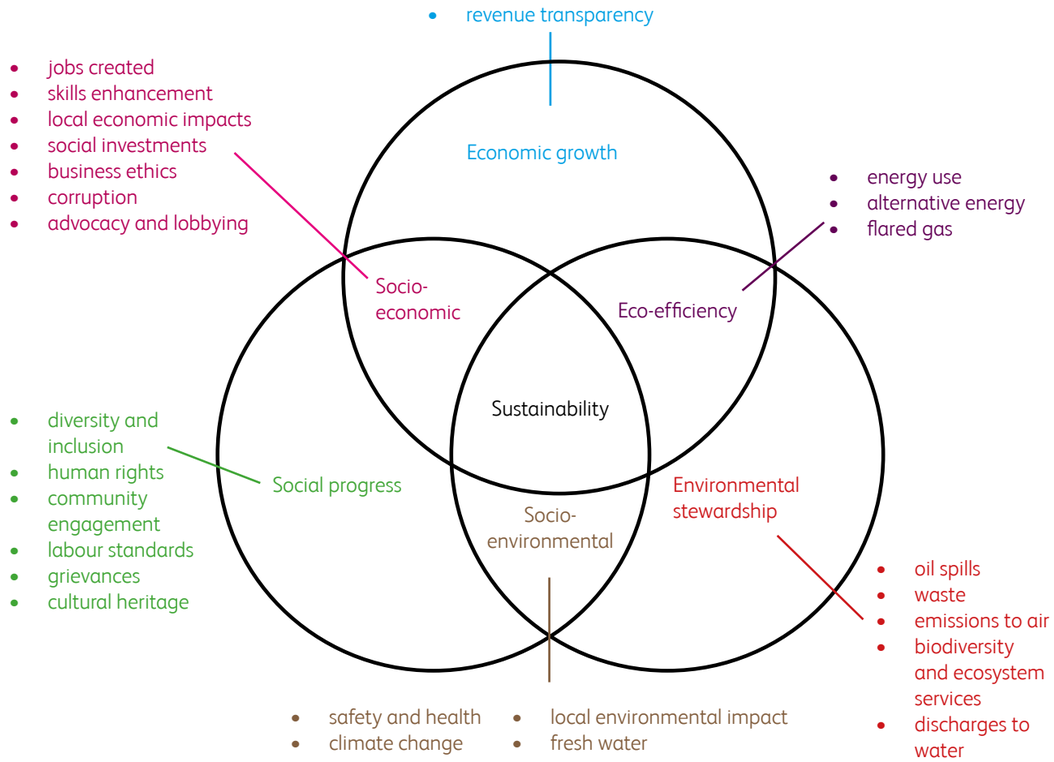
Other risks (UNEP FI's *Environmental and Social Risk Briefing*, 2016) include security of supply and operations, human rights violations, revenue transparency, sustainable community development, community health and safety, and impacts on vulnerable people.

GRI's *Sustainability reporting guidelines & oil and gas sector supplement* (2012) add the following: responding to growing energy demands, contribution to national economic and social development, developing lower-carbon energy sources, transparency, and asset integrity and process safety.

From the numerous sustainability issues confronting an organisation, materiality analysis can help companies identify relevant issues that can materially impact its performance or its stakeholders.

The key material sustainability issues for the sector identified by the industry associations are (Oil and gas industry guidance on voluntary sustainability reporting, IPIECA, 2015):

Figure 2: Sustainability issues



BP had identified the following as material sustainability issues and reported on them (BP's Sustainability Report, 2016):

Our material issues	
Taking action on climate change	• BP's role in a lower carbon future • Natural gas and methane • Renewable energy • Operational emissions
Focussing on safe operation	• Process safety • Personal health and safety • Transportation safety • Security and crisis management
Maximising value to society	• Supporting local development • Engaging with communities • Revenue transparency • Anti-bribery and corruption
Respecting human rights	• Our approach to human rights • Labour rights • Security and human rights
Managing local environmental impacts	• Water • Air quality • Biodiversity and sensitive areas
Foundations for operation responsibly	• Governance of sustainability issues • Our people • Ethical conduct • How we manage risk

It can thus be seen that the nature of risks in the OGI is very complex, diverse and with huge impacts. An integrated business approach, with sustainability at the core of strategy, is absolutely essential.

Integrating ERM and sustainability

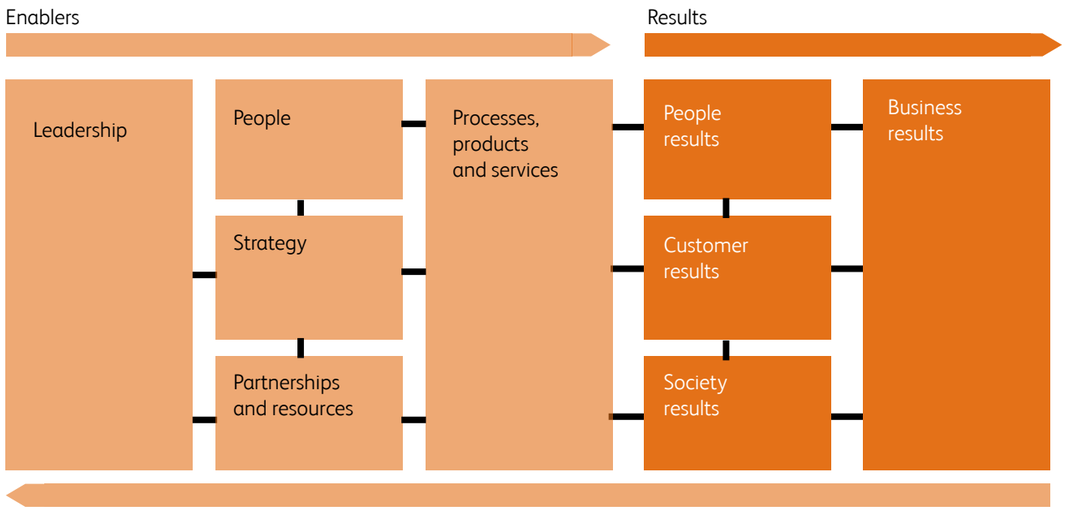
The multiplicity of risks and the enormity of the challenges faced by the OGI perforce call for a concerted effort, right from factoring in all the risks and developing appropriate strategic responses. This eventually mandates a coherent and unified strategy to address the risks in an effective manner. Any piecemeal or compartmentalised approach will only lead to suboptimal performance.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) (*Demystifying sustainability risk*, 2013) also suggests such an approach. While business organisations are quite adept at identifying conventional business risks, they seem to be lacking in addressing sustainability risks.

Pursuing an integrated approach to risk management and sustainability requires an appropriate governance structure. Reliance can be placed on the global excellence models for the purpose. The EFQM Excellence Model (2013), given below (*Figure 3*), is commended as a holistic tool in developing and delivering a stakeholder-focused sustainability strategy.

The Malcolm Baldrige Model for Performance Excellence, widely used in the US and many other countries, is also structured on similar elements.

Figure 3: The EFQM Excellence Model



The objective of the above discussions is to integrate the principles and concepts of sustainability with core business processes and mainstream decision-making in business.

In fine, an excellence journey in sustainability starts with a visionary and committed leadership; is rooted in ethics and values; engages with the relevant stakeholders; identifies all the risks an organisation faces – both internal and external; charts a viable sustainability strategy with clear objectives and targets; provides the required resources; partners with appropriate entities to achieve synergy, scale and speed; implements systems and processes; learns and innovates; and drives results to achieve the desired performance.

The way forward for the oil and gas industry

We are living in a complex and resource-constrained world. The OGI faces daunting risks, some of them threatening its own survival.

The solution lies in holistic management of risks, both from the enterprise and sustainability points of view. Such an integrated approach alone can ensure efficient management of risks and uncertainties, besides enabling the organisations in the industry to seize opportunities, and help in achieving a successful and sustainable energy transition.

"We are good at what we repeatedly do. Excellence is, therefore, a matter of habit"

– Aristotle

What is business continuity management?

Lisa Khan CMIRM

The views expressed are the author's own and do not represent the views of her employer

Business continuity management (BCM) is a framework for identifying an organisation's risk of exposure to internal and external threats. The goal of BCM is to provide the organisation with the ability to effectively respond to threats such as natural disasters or data breaches and protect the business interests of the organisation. BCM includes business recovery and contingency planning.

What is a business continuity plan?

Many business processes are time sensitive, and when an interruption occurs, it is critical that organisations can minimise the impact of the disruptive incident. A business continuity plan (BCP) documents the procedures and resources each department within the organisation will use to keep the business impact to an acceptable level.

Business continuity planning is a mature stage of standardisation reflected in the ISO standards ISO 22313 and ISO 22301. According to industry best practice, all operations should be in scope for business continuity planning. Business continuity planning is one of the components of resilience planning. The other components are emergency response planning (ERP), crisis management planning (CMP) and IT disaster recovery planning (DRP).

Business continuity prepares for the unavailability of the below assets:

- the office, depot or terminal
- the network, power or individual IT applications
- the people (pandemic)
- a disruption in the supply chain (unavailability of a product, contractors cannot deliver)

Accounting for staff is key to the crisis management process, along with safeguarding other assets like IT, telecoms, facilities, access, knowledge and records. It is important to accentuate the importance of vigilance and preparedness throughout the organisation, and to recognise and act to mitigate threats to reputation and assets, but most importantly people. This involves dedication to monitoring external events, careful listening, excellent communication and the willingness to take action early while there is the time to prepare for and mitigate threats.

The energy sector and sustaining business continuity

When it comes to sustaining business continuity, the energy sector faces complex challenges including meeting regulatory demands and managing environmental health and safety issues.

From a strategic perspective, BCM needs to take that one-step-ahead approach to consider potential events that could cause an unexpected loss of operational dependencies (eg offshore infrastructure, people, supplies and services) and the resulting impacts to the business and the wider community. The management of operated assets should include responsibility for ensuring that effective business continuity and contingency plans are in place to respond to events and disruptions that could threaten these facilities, including interruptions to critical equipment and the welfare to protect its people.

The energy sector has seen many business-disruptive events in various geographical areas in which it operates. Crisis management plans are critical where exploration, production and refinery operations are in politically sensitive areas of the world. Examples of other disruptions are:

- dramatic weather events, such as hurricanes and flooding
- terrorist attacks, such as in Paris, London and Brussels
- cybercrimes

In case of such an event a company can decide to invoke the BCPs to protect its staff and business.

Practices to ensure successful implementation

Business continuity planning provides guidelines to limit the extent of impact. It looks at the recovery of business operations so that in the event of a disaster, we can minimise the impact of business disruption. Most of today's leading oil and gas companies can attribute much of their success to properly insulating themselves from business interruption risk.

In your business, it is important to have a risk-based approach to your control framework. Internal control requires managers to establish risk responses to deal with routine risks and to maintain business continuity activities in a range of foreseeable events that can impact business processes or operations. The price for not properly assessing risk often is unanticipated operational downtime.

Business continuity planning is the process of developing procedures and making arrangements for any disaster to enable an organisation to respond to a disaster event in such a manner that critical business functions can continue within planned levels of disruption. Business continuity planning looks at the recovery of business operations, recovery arrangements, manual fallback procedures, alternative workaround and recovery sites. The result of the planning process is the BCP that is appropriate for the office or site (depots and terminals).

Developing a business continuity plan

1. Business impact analysis:

Conduct a BIA to identify time-sensitive or critical business functions and processes and the resources that support them. It is recommended to define business-critical thresholds (impact v time) to determine the scope of your BCPs.

2. Recovery strategies:

Identify, document and implement requirements based on the BIA to recover critical business functions and processes during a disruption.

3. Plan development:

BCP to manage a business disruption that could impact your organisation.

4. Testing and exercises:

Conduct training (tests and exercises) for the organisation to evaluate recovery strategies and the plan.

Business continuity development process

A fundamental component behind the implementation of a successful risk management is the development of an all-inclusive BCP. Given the numerous operational risks that oil and gas companies face, an important first step towards articulating a BCP is an appropriate risk assessment. The plan development process has four stages.

In Stage 1, a risk assessment is conducted to determine the current exposure to disaster risks, the critical processes and activities, the recovery priorities and the recovery time frames.

Using the findings from the risk assessment, a disaster preparedness assessment and strategy is developed in Stage 2 to determine the minimum resources necessary to recover or sustain the business processes and functions and to identify the most appropriate continuity solution based on cost-benefits analysis.

In Stage 3, a BCP is developed. At this stage, the organisation begins to establish the continuity response and develop and maintain detailed continuity procedures. This includes establishing team structures, roles and responsibilities of team members, notification and escalation procedures, contact lists and recovery procedures.

In Stage 4, testing, maintenance and training are required to implement and test the BCP to ensure that the plan will achieve its objectives in a disaster scenario. Regular maintenance of the plan and training processes and procedures are required to keep business continuity planning up to date and ensure a high level of awareness among the staff.

Business continuity planning involves the creation of three documents: a business impact analysis (BIA), a threat assessment (TA) and a business continuity plan (BCP). The organisation needs to identify the areas where it is most at risk and decide what approach should be taken to protect the operation. *See Figure 1.*

Figure 1: Business Impact Analysis flow

The BIA focuses on the activities whose failure would threaten delivery. These tend to be the "operational" activities that interact directly with customers and other stakeholders.

The TA looks at the risks that threaten the organisation's key assets. The nature of risk - defined in terms of its likelihood and impact - will determine which business continuity strategy is appropriate and what, if any, action is required.

At one end of the spectrum, disruptions that have a low likelihood and a low impact may require no specific action and may merely be dealt with generic arrangements. On the other hand, risks that have a high impact and high probability may point to the development of specific plans and risk-mitigation strategies. Or, to put it simple, the creation of a business continuity plan.

What are the overall benefits of business continuity management?

- Optimally recover from a potentially damaging and disruptive incident
- Protect your organisation's turnover, profits and reputation due to improved resilience and preparedness
- Achieve regulatory and governance requirements where BCM is a necessity
- Reduce the cost of business interruption insurance cover based on actual analysis of your organisational risk exposure
- Receive independently audited assurance that your business has established the necessary measures to respond to a potential disaster
- Meet the demands of clients across the supply chain

Other key disciplines

Crisis management planning

CMP is a process by which an organisation manages the wider impact of a crisis until the crisis is either under control or contained without impact to the organisation. A crisis is defined as a situation that falls outside normal BCP and emergency response arrangements and potentially threatens the safety or well-being of the people, the environment, the company's reputation and/or its financial bottom line. Ultimately, it may put your company's licence to operate at risk.

IT disaster recovery planning

DRP focuses on the recovery of computer systems and network or IT infrastructure and applications, which are referenced within the overall planning process, together with detailed IT recovery processes.

Emergency response planning

ERP deals with operational incidents that require swift action by the business in order to minimise casualties and damage to the environment (and herewith the operational disruption). The emergency response relates to the initial immediate actions required to stabilise the health and safety aspects of such operational incidents.

People should be at the heart of business continuity planning

No organisation can function without its people. During and after a crisis, it is the resilience of the people that make up an organisation's community that gets it back on its feet and working again. It is important to know that all employees have a part to play in business continuity planning. As a staff member, you are required to become familiar with business continuity policies and procedures. In the event of an incident, follow guidance and remember to report any business continuity weaknesses to your local business continuity focal point.

Online research articles reference

- **Business continuity management (BCM) -** https://searchcio.techtarget.com/definition/business-continuity-management-BCM
- **What is a Business Continuity Plan?** - https://www.everbridge.com/solutions/anticipate-and-prevent-disruptions-to-operations/business-continuity-planning/
- **Operational Risks Justify Oil & Gas Business Continuity Planning** - https://blog.schneider-electric.com/power-management-metering-monitoring-power-quality/2017/09/08/operational-oil-gas-business-continuity/
- **Why People Should be at the Heart of Business Continuity Planning** - https://www.thebci.org/news/why-people-should-be-at-the-heart-of-business-continuity-planning.html

The lean start-up - a new approach to implementing portfolio contingency management

Peter Smith CMIRM

Partner at QuantPro, Risk & Controls Consultancy

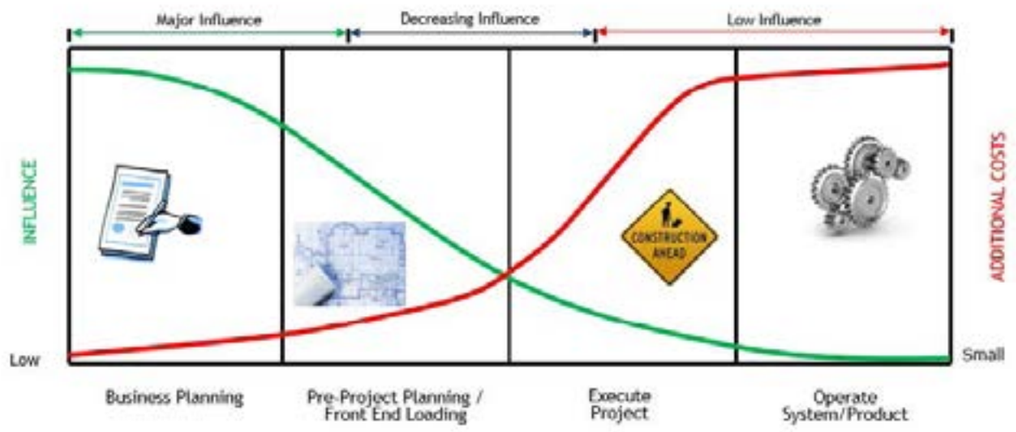
Risk management influence

Now that the oil markets are beginning to stabilise and even rise above that coveted $70 mark, there is a palpable shift in mood in the oil and gas industry and as such a renewed focus on new projects, so it is therefore vital for risk management focus to shift to developing a best-practice approach to managing risk across a portfolio of projects from new ones to existing. By establishing a definitive risk management process and decision-making tool at the beginning of this new period of project "start-ups", a stronger and more certain portfolio can be established, minimising uncertainty and risk, and allowing higher-risk projects to be taken on for those higher rewards.

There is an age-old influence v cost matrix in risk management (see below), and it applies in this instance as much as it ever does. Writing a decision-making process, change control process and the appropriate risk management procedures has minimal cost, but the long-term effects of an effective portfolio risk and contingency management process can be worth millions in mitigated risk and opportunities seized.

However, a major barrier to starting a process is the inherent human psychological setting that a product, a procedure, a plan must be complete for it to be put in place. In order to gain quick buy-in, we must have the perfect product to drop in with minimal effort or disruption to the system. However, this is rarely the case with any service or product so another approach to gaining buy-in must be taken. This is where I believe the "lean start-up" approach favoured by tech start-ups and Silicon Valley can be taken in order achieve an eventual working "portfolio contingency management process".

Figure 1: Risk Management Influence Chart



The lean start-up

The lean startup is a book by Eric Ries which is primarily aimed at tech companies and product developers. However, in recent years working in projects and attempting to introduce change and especially a contingency management process where none exists, I see it more and more as a valuable method of rolling out new services and processes in projects and enterprises to combat the resistance to adoption of something new. Eric describes how rolling out a product that isn't the complete finished article with all bells and whistles allows those who embrace innovation to test it out and provide valuable feedback while others will hold off until the "mass adoption" phase.

Figure 2: Technology/Innovation Adoption Life Cycle

Take examples such as Tesla and Facebook. The Tesla that is gaining traction today and well placed in the "early adopters" stage is not the Tesla that first hit the market years ago with only innovators purchasing. Facebook's innovators were the college campuses of Harvard and the like, before it was also taken up by early adopters across the country, followed by the international breakthrough as the early majority took up the use of Facebook at a steep trajectory until now, when we are well past the mass majority in the billions of users, and the "laggards" are left.

If we apply this to a portfolio of projects in a large organisation, we can look at it in two ways. Is your organisation itself an innovator or early adopter of contingency management?

Figure 3: Project Innovation Adoption

Or will it be the late majority or laggard? The famous example of a company which was on the wrong side of the curve is Nokia and its movement on the smartphone revolution. Based on my experience in risk management over the last 12 years or so, I would suggest that the current "portfolio contingency management" status is at the early adopters stage as many companies talk the talk, but as a working process, they rarely walk the walk. I have been lucky enough to work with two companies I would thoroughly put in the innovators category and helped roll out such a process.

The second way of looking at the adoption timeline is internally with individual projects, especially as we move into a phase of new projects starting up. Can we say that Project X will be the innovator for future projects and even projects which are already up and running? Can we roll out an MVP (I'll explain this shortly) on a new Project X to start the process and lead the way to early adoption and then mass adoption?

The process of developing an MVP (Minimum Viable Product) allows us to get in early on the influence line and low on the cost line to test out the product and make enhancements along the way before that critical mass adoption phase where, if the product isn't the complete package, it may fail. This is vital for implementation of a functioning portfolio contingency management process. To ensure a buy-in to roll out contingency management on each project to then form a portfolio process requires evidence of a working product and not just a theory; it requires the innovators and early adopters to be talking of the benefits and stoking the interest of the majority. It works in tech (Apple), in food (avocados), in industry (renewables) and can do so in risk management.

Minimum Viable Product (MVP)

Building an MVP is a lot more palatable than building the final end product for mass adoption; it allows a small bite to be chewed before the company has to try to swallow the whole pie. So in the case of new projects we build an MVP for contingency management that is project specific. That process involves:

- calculation of contingency
- implementation of a change control process linked to contingency drawdown
- monitoring of risk exposure v contingency remaining
- lessons learnt reviews

Contingency calculation

The first step in the process is the calculation of project contingency. Contingency is "an amount of funds added to the base cost estimate to cover estimate uncertainty and risk exposure" (PMI, PMBOK, 2017), and as such should be calculated through the process of probabilistic analysis of the cost estimate uncertainty and discrete risks events. This calculation begins at the stage 1/Class 5 estimate and would follow guidelines such as the AACE/ RACI estimate uncertainty ranges such as the below around the cost breakdown structure (CBS) and cost items in the estimate.

Cost estimate classification	Level of definition (% of complete definition)	Cost estimating description (techniques)	Expected accuracy range
Class 5: Order of magnitude	0% to 2%	Stochastic, most parametric, judgement (parametric, specific analogy, expert opinion, trend analysis)	L: -20% to -50% H: +30% to +50%
Class 4: Budget	1% to 15%	Various, more parametric (parametric, specific analogy, expert opinion, trend analysis)	L: -15% to -30% H: +20% to +50%
Class 3: Preliminary	10% to 40%	Various, including combinations (detailed, unit-cost or activity-based; parametric; specific analogy; expert opinion; trend analysis)	L: -10% to -20% H: +10% to +30%
Class 2: Intermediate	30% to 70%	Various, more definitive (detailed, unit-cost, or activity-based; expert opinion; learning curve)	L: -5% to -15% H: +5% to +20%
Class 1: Definitive	50% to 100%	Deterministic, most definitive (detailed, unit-cost, or activity-based; expert opinion; learning curve)	L: -3% to -10% H: +3% to +15%

Figure 4: AACE Guidelines, 2017

In addition to the uncertainty ranges, the analysis would include discrete risk events modelled as appropriate taking into account the probability of occurrence and the possible cost impacts (three-point, Minimum, Most Likely and Maximum being the most common at MVP stage). The analysis combining both uncertainty and risk will give an output of confidence ranges from which a decision can be made as to the setting of contingency levels based on risk appetite, project specifics and project stage. These three elements will also be the basis for a decision to add a provision for "unknown unknowns", which can often be added as one standard deviation from the analysis output but will never be an exact science due to the nature of "unknowns".

Project change control

With a contingency set from the output of analysis, contingency management is often where best practice falls by the wayside as additional scope and design and stakeholder changes creep into the project. Without the relevant processes and procedures in place, contingency is swallowed up and the project ends up in trouble, posing a wider risk to the portfolio and company as a whole. With a new project will come a new Project Execution Plan (PEP) planning out how the project will be managed. In this, the change control process is set and should include a clear and transparent procedure with delegation of authority for request for changes from the baseline.

If we estimated steel beams would cost $1 million but at time of procurement the cost was $1.1 million, then we must submit a request for $0.1 million to be drawn down from contingency. If the original uncertainty analysis was carried out correctly, then there could well have been an amount of uncertainty identified within the CBS and therefore should be linked as such in the request for change (variation order). This equally applies for the drawdown from contingency for discrete risk events. Costs associated with mitigation actions or for the impacts of risks should be linked in the request for change which could be as simple as Change Request ID to Risk ID or CBS level or, of course, in some instances it may have been an unforeseen event but this should be noted for lessons learnt.

However, it is important to note that an amount may not be the exact correlated drawdown amount as it may be more or less than what was originally estimated in the contingency analysis. This is why we use multiple thousand iterations and calculate contingency at a Mean, P80 or even P90 level as some risks and uncertainty provisions may not be required, whereas others may be required at the maximum level or more. The process should remain the same, however, and this sort of information fed into the lessons learnt stage.

A rigorous and transparent change control process will ensure additional scope, and non-conventional change can be rejected and contingency protected for what it is intended for and therefore better serve the project.

Risk exposure v contingency

A periodic (monthly or quarterly) tracking of risk exposure through an updated run of the risk analysis process will allow the exposure to be plotted against the remaining contingency and drawdown to establish if the project is over or underexposed, which facilitates responsible and informed decision-making on contingency drawdown and project risk as well as feeding a vital component of the future portfolio-level decision-making.

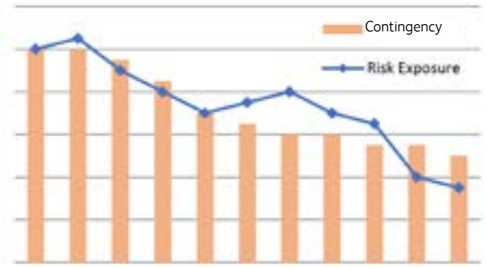


Figure 5: Contingency Vs Risk Exposure Chart

Lessons learnt

The audit trail provided by the initial and continuous risk analysis and contingency drawdown via change control acts as a natural lessons learnt document which can be formally combined with a lessons learnt review and documented. Did we have sufficient contingency? Did actual risk impacts fall within our estimates? Did we sufficiently manage risk? Which CBS areas did we overestimate or underestimate? These are all valuable lessons for improving future project estimation, scheduling and risk management.

Product 2.0

The next stage in product evolution, following feedback from innovators and early adopters, will be the introduction of enablers for the final product and mass adoption with the target being a comprehensive portfolio-wide contingency management process. Enhanced Feature number one is the introduction of "management reserve".

Project contingency v management reserve

The distinction between a project contingency and management reserve is often confused, yet the titles are self-explanatory. Project contingency is owned by the project and therefore, although governed by a defined change control process and tracked through the management of change, should be managed by the project manager and commercial manager at that level to deal with discrete risks (breakdown of critical rigs) and uncertainty within the project estimate (quantity or cost changes) and schedules (durations).

Management reserve is an amount set aside and held at senior management level (portfolio director, board, etc) to be drawn down only in the instance of a significant "black swan" event or if the project is in significant difficulty and is deemed critical. How this is split will depend on the risk appetite of the company, project or portfolio, but a common and introductory standard approach for non-complex projects would be Mean confidence level set as project contingency and P90 minus Mean is set aside for management reserve.

Portfolio contingency management

Following the introduction of project contingency management on the initial innovator project, then early adopter project, the management reserve introduction has now enabled the early majority of project to undertake the process of change to implement contingency management on their project with appropriate processes and procedures in place and company experience.

Managing a portfolio of projects with varying risk profiles (exposure v contingency remaining) and Internal Rates of Return (IRR) requires a juggling act of cash flow and decision-making. A portfolio contingency management system aims to make decision-making and balancing projects at different stages, sizes and performance levels simpler by pooling management reserve from each project to be held as contingency to hedge for poor-performing projects against the success of others. This is particularly vital in the high-risk world of exploration and drilling projects where projects can be abandoned if the tight success margins of a business case are broken by the cost increases and delays associated with poor risk management. The management reserve also acts as a cash-flow buffer to provide additional stability; it is a form of high-level enterprise risk mitigation for the risk associated with taking on new projects.

The management reserve split of a contingency calculation project is held in the portfolio reserve, and a tight controls procedure with a higher level of delegated authority, often at board or C-suite level, is put in place to ensure that if a project has to submit a request for additional drawdown from management reserve to cover spiralling costs associated with uncertainty, risks or unforeseen events, then it has to go through due process.

This due process should take into account the portfolio as a whole with Net Present Value (NPV) calculations and as such IRR as well as current risk profile of each project taken into account. This way a simple drawdown can be taken from the pool if the general state of the portfolio is healthy across the board, or a decision can be made on pulling out of a project that isn't viable and isn't worth risking the ability to cover more profitable and strategically important projects.

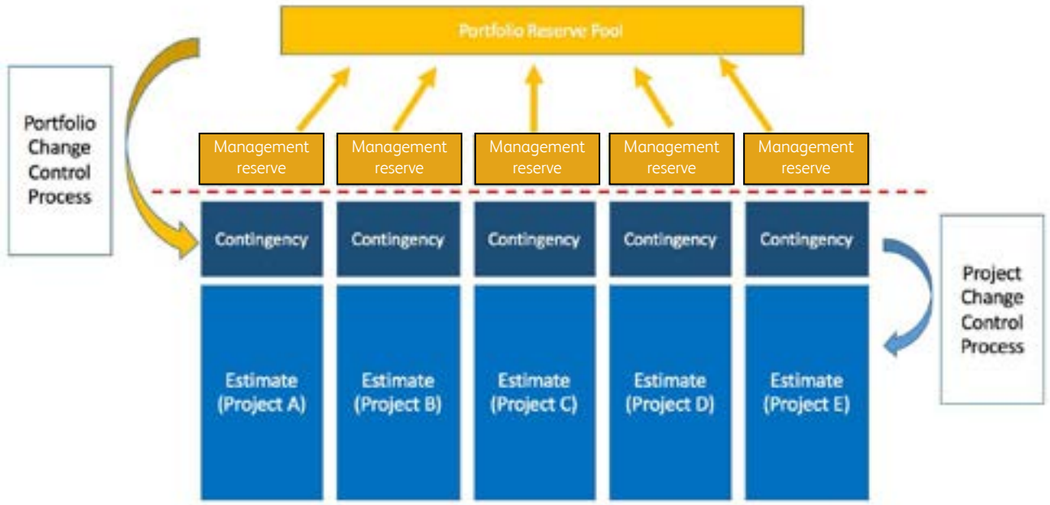


Figure 6: Portfolio Contingency Management

An example based on the above diagram would be that Project A hits significant trouble and requires additional funding to ensure it can be completed. An assessment can be made with regard to drawing from the portfolio reserve pool. Firstly, the project would provide a full justification of the funding requirements for the portfolio board/panel to review. Then reviewing the portfolio across projects B-E, taking into account criteria such as current performance, current stage, estimate value, risk profile trends, historical drawdown and IRR as well as external influences, the panel can make a decision on funding from a portfolio drawdown.

Early adopters

If your company can go through the lean start-up process internally, developing innovative and early adoption in new projects, followed by staged roll-out of additional features aimed at mass adoption in order to introduce a portfolio contingency management process complete with risk analysis procedures, change control procedures and defined risk appetite and strategy, then it will firmly place itself as an early adopter on the curve and allow itself to take on new projects with renewed confidence of success through effective management of risk at both project and portfolio level. Risk management, like modern tech start-ups, is as much about the perception as it is about the product when it comes to adoption.

Survey Results part II: Risk management maturity

Organisations were asked to consider their maturity in terms of different aspects of risk management and, unsurprisingly, technical safety and security ranked highly (see: *How mature is the company in the following areas?*) Respondents identified both ERM and business continuity as their weakest areas.

The survey's high-level snapshot of risk maturity in the industry found that the large majority of organisations (over 70 per cent):

1) Have a risk policy and procedures in place
2) Qualitatively assess corporate risks on a regular basis
3) Ensure risk mitigation was in place for all key risks
4) Use risk management as part of decision-making
5) Use cost and schedule risk analysis for projects
6) Have business continuity plans "somewhat" in place

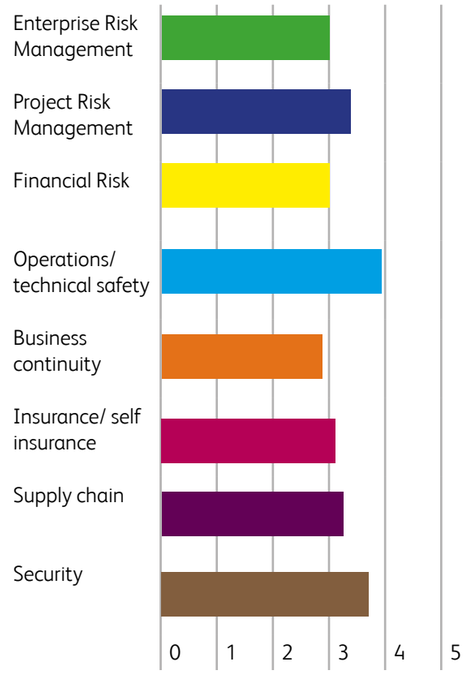
In addition, a majority (over 60 per cent) of organisations had:

1) A risk committee in place
2) Output from various projects which is reported and used to a degree, to understand the overall project/ asset exposure to the company

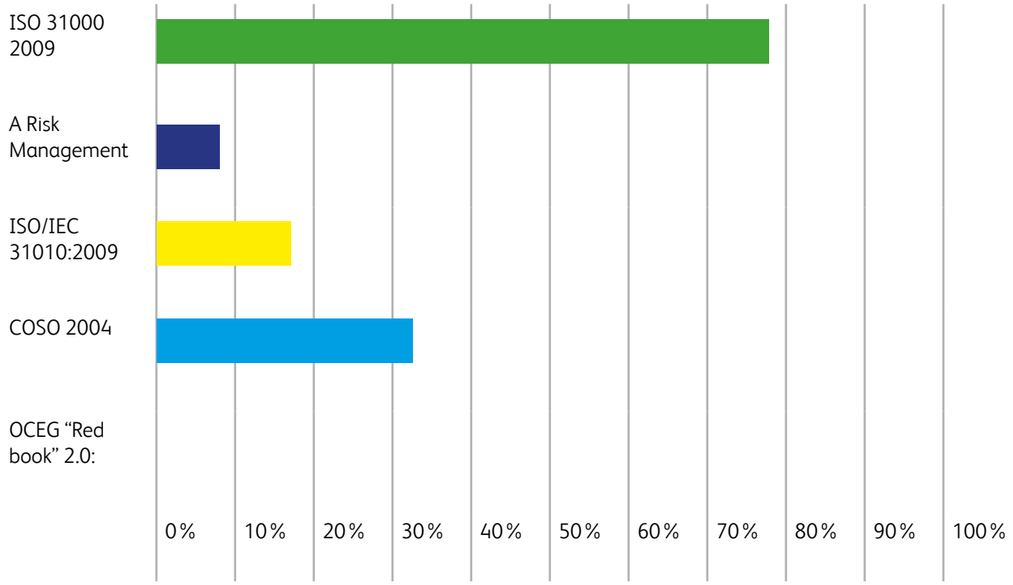
The general survey findings were that risk maturity within the industry was at level 3 – established. Domenic Antonucci describes this as "… disappointing for a sector with the history, sophistication, management talent and resources of oil and gas," in *Moving up the risk maturity curve for the oil and gas sector* (pages 37-41).

How mature is the company in the following areas?

(1-5 where 5 is very mature)

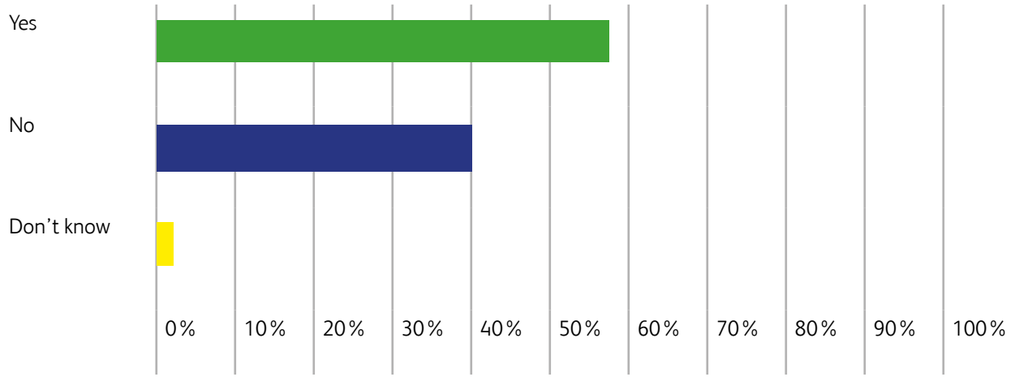


Do you specifically follow or have you designed your risk management programme based on any of the following standards?



Risk maturity matrix

Have you developed, or do you use, a risk maturity matrix?



Most respondents said that they tended to follow ISO 31000 when asked, *Do you specifically follow, or have you designed your risk management programme based on any of the following standards?*

Over 50 per cent of respondents said they were using a risk maturity matrix to either measure themselves with or to create a roadmap for their risk management programmes (*Have you developed, or do you use, a risk maturity matrix?*).

Having a risk maturity matrix with levels from, for example, 1 to 5, allows the effectiveness of and improvements to a risk programme to be tracked over time. It can also be used to measure the maturity of different subsidiaries or departments or regions.

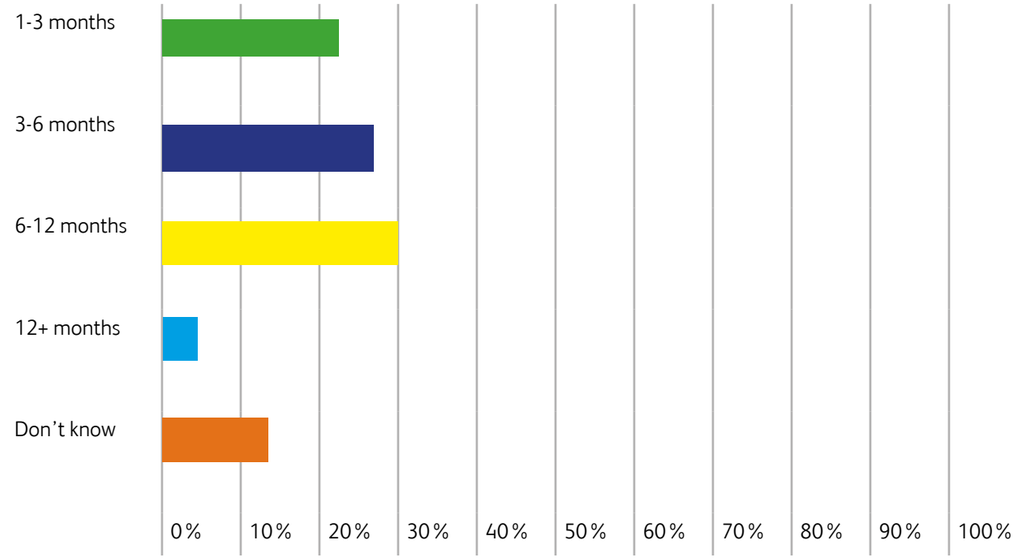
It can also be used to measure the maturity of different subsidiaries or departments or regions. Armed with an understanding of the organisation's current maturity, senior management can provide guidance as to what level of maturity the organisation aspires to reach. The gaps between the current level and aspired level of maturity therefore become the actions needed to be taken, essentially a roadmap for risk management. Since the majority of respondents said they were using ISO 31000, Antonucci's advice on how to measure risk maturity against that standard is timely.

Risk management information

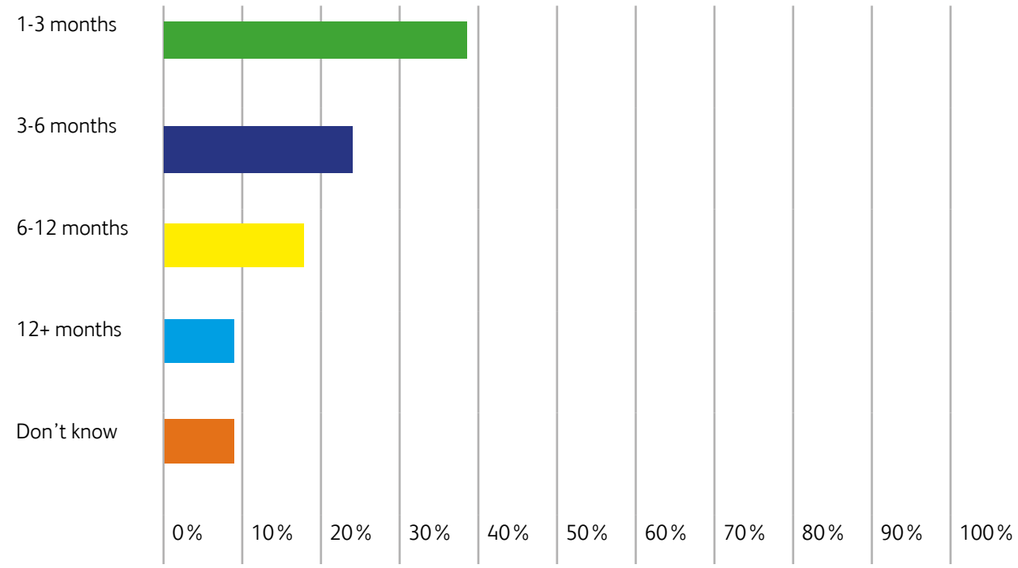
The survey sought to discover how confident organisations were that their board receive sufficient, regular, transparent and robust information on risk. Half said they were, but 30 per cent said they were not very confident, and 20 per cent that they were unsure. This indicates that improvement needs to take place either in the quality of risks captured, the escalation and consolidation process involved, or in risk reporting.

Ideally, while organisation's should report risks on a periodic basis, more importantly, it should be live and relevant and risk management should form part of all decision making. It is therefore encouraging that at a corporate level, one in five respondents said they reported more than four times a year (*How often are risk registers updated at a corporate level?*). A further quarter said they did so between two and four times a year – the majority either half-yearly or annually. It is important to note that reporting is not necessarily an indication that the risk data is being used effectively. It was interesting to find that more than 25 per cent were reporting between two and four times a year, and even more interesting was that more than 20 per cent were reporting even more frequently than that. Departmentally, as expected, most report on a regular basis (*How often are risk registers updated at a departmental level?*)

How often are risk registers updated at a corporate level?



How often are risk registers updated at a departmental level?

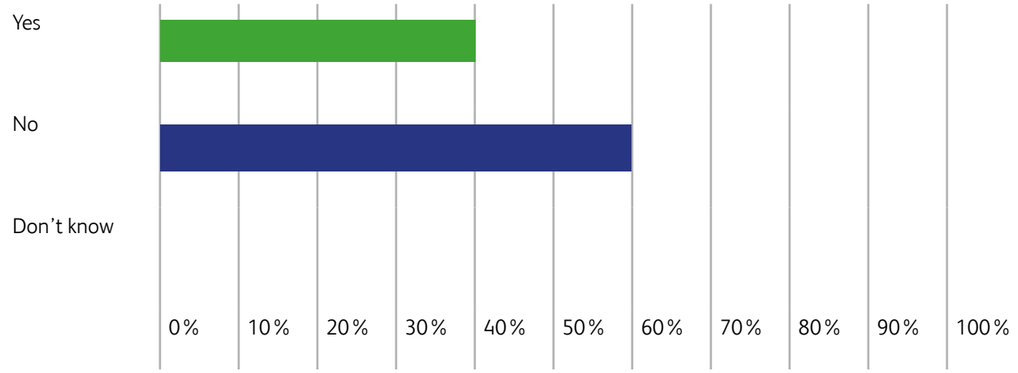


Risk software

Considering the size of the organisations in question, the expectation is that ERM software would be in place and would be actively used for reporting and analysis purposes – but almost 60 per cent of those surveyed did not use ERM software.

Such software may not be better at helping risk managers report and analyse risk. However, in the free-form sections of the survey, several commented that not having ERM software posed a challenge to implementing risk management across large organisations.

Do you have an Enterprise Risk Management software solution?



A risk management information system (RMIS) is software used to capture and store risks, evaluate them and keep track of associated information. Most software includes a level of automation to set reminders for risk and action owners. Alongside being an effective database, it can also be used to provide effective risk reporting and dashboards for key staff.

The benefits include:

- **Data**: RMIS helps reduce redundant data and prevent data errors, while also ensuring version controls.
- **User friendliness**: Excel, which tends to be the software of choice when creating risk registers, is often not user-friendly and many are reluctant to use it. This can hinder progress of risk management and a risk software can address this.
- **Silos**: Using Excel or other less sophisticated software makes it difficult to share risk information in real time. RMIS allows users to access other department or projects risks which increases communication and quality of the risks identified.

The drawbacks include:

- **Data**: Data is only as good as the risks captured. If an organisation has a poor risk culture or awareness of risk, the software may become a repository of issues or challenges rather than risks.
- **Framework**: Often, companies implement software before having fully developed their framework. When this occurs, the software can end up influencing how risk management is undertaken with reference to culture, structure and processes, for example, leading to it being ineffective.
- **Cost**: Software comes with a price, and while the one-off price may be considered, the ongoing costs of licences, support, changes to the software, updates and time (training, administration, etc) can be underestimated.

One of the best ways to engage top management and support decision-making is through risk visualisation, according to *Better decision-making through risk visualisation* by Nico Lategan (pages 42-44), Head of Enterprise Risk at Transport for London and an expert in the field. This may be done with or without risk software and is more important in building a strong culture and ensuring risk-based decision-making and top-level support.

	NO	1	2	3	4	5
Risk culture is embedded throughout the organisation	9.38% 3	3.13% 1	28.13% 9	21.88% 7	25.00% 8	12.50% 4
People are educated on the importance of managing risk	6.25% 2	6.25% 2	21.88% 7	28.13% 9	18.75% 6	18.75% 6
Risk management and Internal Audit complement each other	9.38% 3	12.50% 4	12.50% 4	28.13% 9	15.63% 15	21.88% y
Risk management training is provided across the company	18.75% 6	12.50% 4	12.50% 4	25.00% 8	18.75% 6	12.50% 4

Risk culture and training

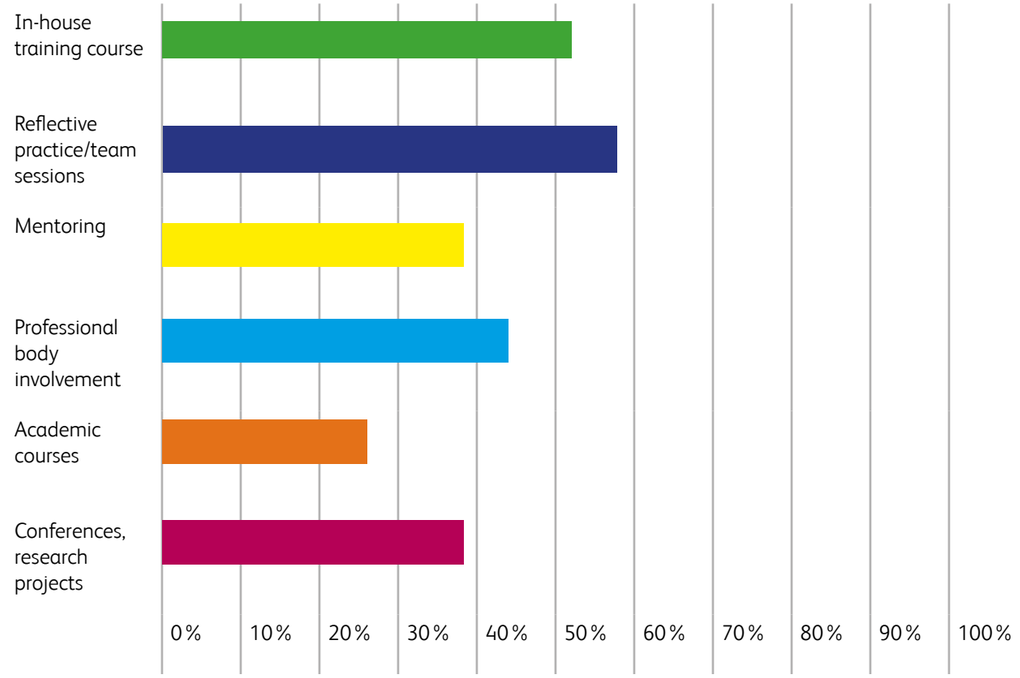
The survey found that just over 37 per cent of organisations said that risk culture was embedded throughout the organisation (see *Risk culture*). But there was also some frustration, from a lack of general understanding across the organisation of what risk management is, to a lack of communication from senior management. Compliance is an issue too, with many seeing risk management as a compliance tool due to the culture of the company.

Risk culture plays a fundamental part in risk management – from the risk maturity of the organisation to the decision-making process and the success of implementing an effective risk management framework, as Horst Simon discusses in *Risk culture building* (pages 45-47).

Training

A key aspect of risk culture is that of training. A positive trend in the industry is the dedication to ongoing risk education. Organisations take advantage of a number of approaches (*How do you ensure you and your team are up-to-date with risk frameworks and the current risk environment?*) The most popular approaches are in-house training courses and reflective practices and team sessions. Mentoring, professional body involvement, conferences and academic courses are all being utilised heavily by organisations.

How do you ensure you/your team are up-to-date with risk frameworks and the current risk environment?



In-house training courses tend to be equally split between internal and external training with most training budgets set between $5,000 and $25,000, according to the survey.

Challenges to implementing risk management

Respondents raised the following issues in the free-form answers to the survey:

- **Resources**: Many said risk departments were often understaffed or, where there were enough staff, there was the risk of losing key members of the department. The skills gap made it difficult to fill key roles, they said. Some added that a lack of risk competency was often evident when it came to building a risk champion network across an organisation.
- **Budget**: Many risk managers said budgets were too stretched, which may explain the lack of risk software investment as well as the lack of resources.
- **High-level visibility of risk management**: Risk managers said they sought more visibility and independence. This can indicate a lack of the right tone at the top. Many boards are not necessarily equipped with the level of risk management knowledge that is needed. Where risk understanding is evident, there may not be the mechanism in place for them to be seen to be using risk management.
- **Risk appetite**: A few respondents said there was a lack of an effective risk appetite within the organisation. From risk maturity and project risk to risk culture, risk appetite was consistently mentioned as an important tool to aid decision-making. Alexander Larsen CFIRM, president of Baldwin Global Risk Services Ltd, sheds useful light on the topic in *A more effective approach to risk appetite*, pages 48-51.
- **Reputation**: While the issue of reputation was not explicitly addressed by the survey, it was raised as a key risk and focus area in a number of comments by participants. Since any accident or incident could have a major impact on reputation, it has become a major topic of discussion in the industry. Hans Læssøe discusses how companies can manage their reputational risk in *A more effective approach to risk management* (pages 52-54).

Moving up the risk maturity curve for the oil and gas sector

Domenic Antonucci CMIRM CRISC

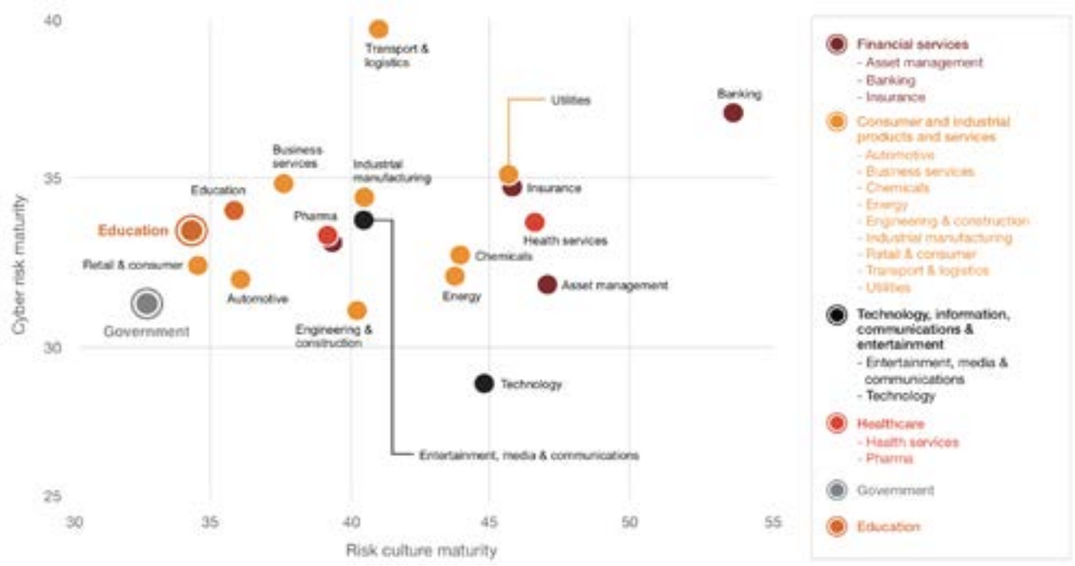
Interpreting the IRM risk maturity results

The IRM survey section for risk maturity suggests room for improvement by the oil and gas (O&G) sector. The self-assessment ratings seem to be at a "middling" maturity level. This is disappointing for a sector with the history, sophistication, management talent and resources of O&G.

As an ex-Shell planner, I feel a little embarrassed by the survey results. Even more so because if we discount the non-facilitated ratings for Optimism Bias by, say, 20 per cent, then the IRM survey results may look worse. Look below at our Figure 1 sector comparison by PwC for the "Energy" sector; it also suggests that O&G are lagging for both ERM and cyber-risk maturity.

Figure 1: Industry risk maturity by ERM and by cyber.

Source: PwC client survey, 2017



So, what to do? Suggest how to improve, that's what!

Let's remind O&G of the "hard" benefits of risk maturity and suggest how to maturity-benchmark better against self-improvement, or sector, or codes (such as ISO 31000 as preferred on the IRM survey by O&G) and by cybersecurity maturity.

"Hard" benefits proven for moving up the risk maturity curve

Firstly, the O&G sector should get up-to-speed with the proven research track record over recent years of the "hard" benefits (not just the "soft" benefits) for higher over lower risk-mature firms. The two summary Figures 2 and 3 are a start and may motivate O&G to move further up the risk maturity curve:

If the below is not enough to motivate O&G, then perhaps recourse to compliance obligations will. The Institute of Internal Auditors (IIA) has mandated the assessment of ERM effectiveness (at least annually) and has linked this not only to an ERM maturity model but also to ISO 31000.

Figure 2: Risk maturity comparisons

Source: E&Y & FERMA Global Risk Report, 2011

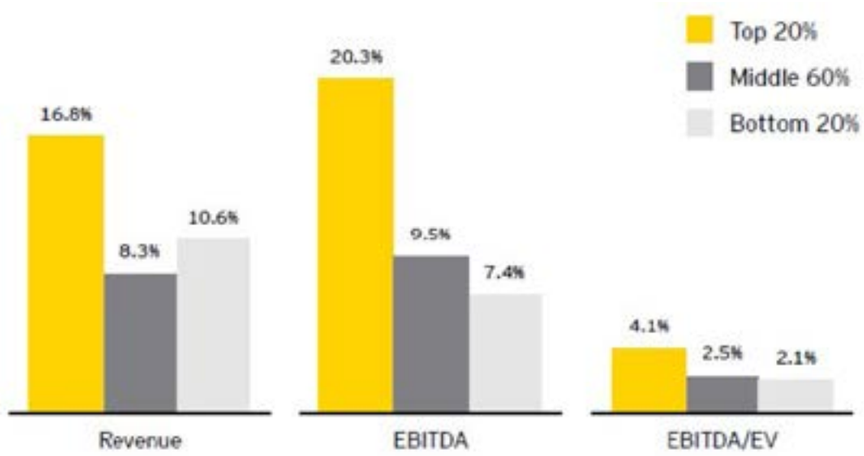


Figure 3: Further risk maturity comparisons

300%	Headlining EBITDA gains by top 20% high-mature v bottom (E&Y & FERMA, 2011)
10%+	Revenue gains by 29% of higher firms v 18% for lower (FERMA, 2012)
+25%	Firm valuation gain by Tobin's Q method (Farrell, M & Gallagher, R, 2014)
23% and 48%	Project cost savings & schedule savings (Hopkinson, 2012)
11%	Return on asset performance gains (Aon, 2014)
50%	Stock price volatility reduction (Wharton & Aon, 2012)
28%	Operating margin gain over plan (Aberdeen Group, 2014)
17%	Compliance cost savings over past two years (Aberdeen Group, 2014)

ISO 31000 risk maturity strengths and weaknesses

A strength of ISO 31000 is that it requires organisations to develop strategies to improve their risk maturity strategy alongside all other aspects of their organisation.

As Kevin Knight, the "Father of ISO 31000", says: "Risk maturity models are powerful tools to affect such strategies".

Few people realise that ISO 31000 implies its own risk maturity model. This has fifteen capabilities grouped into three levels, as in the table below:

Figure 4: ISO 31000-implied risk maturity model capabilities table

Source: www.iso.org

Generic level	ISO lexicon	ISO refers to capabilities in...
Advanced	"Enhanced attributes" Annex	n=5: Key outcomes, continual improvement, full accountability of risks, application of RM in all decision-making, continual communication, full integration into governance structure
Intermediate	"Organisational arrangements" for managing the risk framework	n=7: Risk management plan, external communications plan, internal communications plan, people accountable, tools and techniques, resources allocated and policy/procedures/ practices
Basic	"Foundation components"	n=3: Top mandate and commitment, clear risk management objectives and integrated governance

Unfortunately, ISO 31000 is not enough in terms of covering all the maturity capabilities required of a modern organisation. Good practising chief risk officers know this. Within my Benchmarker™ risk maturity model, for example, both ISO 31000 and COSO ERM barely cover two thirds of the capabilities required.

So, O&G firms should be warned if they only aspire to align with either ISO 31000 or COSO ERM.

Benchmarking against sectors

There seems to be more "talk" than "walk" about the use of benchmarking against other sectors. O&G firms have indeed commissioned consultant reports. For example, Kuwait Petroleum Corporation (KPC) used to show one they commissioned at conferences several years ago.

However, even if results such as those in Figure 1 may capture senior management attention, this attention is typically fleeting. The practical realities are that robust external data is difficult and expensive to obtain, it is rendered out-of-date quickly and is often challenged as "not relevant to us" by management.

Benchmarking against codes

More useful is benchmarking risk maturity against leading international reference codes. For ERM, the leading three are ISO 31000:2009 standard, COSO ERM 2004 guidance and King Code III:2009 principles. King Code is included because of all the world's corporate governance codes, this one gives the most specific details for ERM over any other – and some that the other two do not cover.

From my research and book, there are over 48 ERM risk maturity models in the market. None are created equal. Most are proprietary. All have some bias or other. Some have little more purpose or substance than to act as a "teaser" to sell insurance or other products. Many can be used in tandem. And some are very useful.

The question for O&G is: what are my needs to continue moving up the risk maturity curve in terms of a risk maturity model solution? To kick off any needs analysis, I offer a table over the page from the research that went into my book. The table's empty cells indicate NO or NOT PUBLICLY KNOWN. Excuse my own self-confessed bias for my own Benchmarker™.

Need for...	Benchmarker™	G31000 RMM draft	Logicmanager RIMS 2006	Other maturity models
ISO 31000:2009 cross-referenced	Yes			
ISO 31000:2009 aligned	Yes	Yes		Several
COSO ERM 2004 aligned	Yes		Claimed	
King Code III aligned	Yes			
CRO-content added/aigned	Yes	Yes		
CRO practitioner authored	Yes			
Metrics for multiyear roadmap	Yes			
Robust internal rating method	HB158 adapted			
Software version	Yes		Yes	
Designed to drive risk management plans	Yes			
IIA mandate satisfaction	Yes	Yes		
Avoiding bias to one code	Yes			
Risk culture content rich	Yes			

Benchmarking against self-improvement

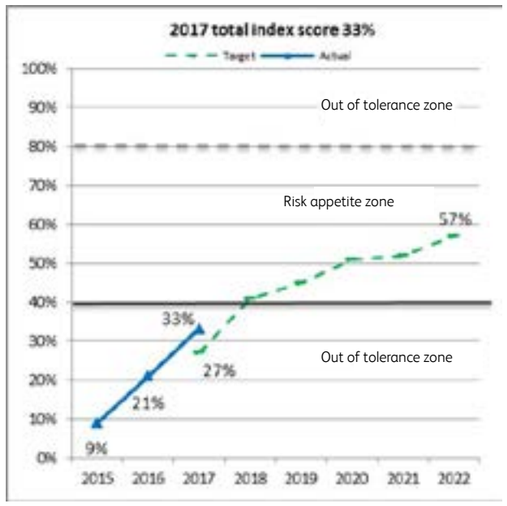
Nevertheless, the most useful, easy and practical of all approaches is to benchmark risk maturity against self-improvement from a baseline over multiyear time AND use the top three reference codes above as well. Of course, this requires a working model with robust metrics that puts an implementation "engine" behind the now-tiresome five-scale maturity slide-bar … I still recall one conference presenter telling me his slide-bar was "intuitive" with nothing behind it … *spare me!*

Even better is to take the outputs from the annual maturity reassessments as a five-year roadmap and use them as the core content to drive the annual risk management plan. Most risk management plans I've come across are ad hoc and "make-it-up-as-we-go-along" by the risk function. Far more powerful plans know they are delivering maturity gap improvements in the right direction year-after-year with interfunctional input from the maturity reassessments.

It does not matter where your O&G organisation currently sits – you can always keep moving up the risk maturity curve. Here's a sample of Firm A using an S-curve graph to report to board and senior management how they benchmark their actual self-improvement against targets on a rolling five-year roadmap.

Firm A's risk appetite is to keep moving up the risk maturity curve beyond the pack of organisations who underperform and head towards the high-maturity organisations up around 80 per cent index. However, they realistically understand that within five years they may not have the resource to quite get there – but these targets will be reviewed with the roll of each year's plan.

Figure 5



And then there is cybersecurity maturity

Let's look at the PwC Figure 1 again.

For O&G firms wanting an easy-to-use cyber-risk maturity model with an Index percentage score metric, then start with the Epilogue of the *Cyber risk handbook*. Here, 25 subject matter experts from around the world have summarised the cybersecurity capabilities expected (by the CEO and board) from every key enterprise function in the modern organisation. They answer the question often begged:

If cyber-risk management is not just an IT risk but an enterprise-wide risk, what function-by-function capabilities do we need?

For example, one Gulf NOC swore they were at about "85 per cent good" for ERM maturity. They were shocked when they self-rated as 51 per cent Index on my Benchmarker™ risk maturity model.

Notes: Most of the references in this article are sourced from the author's two books entitled *Risk maturity models: how to assess risk management effectiveness*, Kogan Page UK, 2016, and *The cyber risk handbook: creating and measuring effective cybersecurity capabilities*, Wiley NY, 2017. As per the IRM study, the codes referred to in this article do not take into account the most recent updates by all three codes.

Better decision-making through risk visualisation

Nico Lategan

Head of Enterprise Risk, Transport for London

There are many elements at play in making good decisions. These can include the effect of biases, the importance of options evaluation, the ability and a commitment to follow through and the role of power dynamics; however, this article will focus on how having timely and accurate information presented visually can inform better decisions. This includes information on:

- objectives (what are we trying to achieve?)
- strategy (how are we going to get there?)
- performance (how are we currently doing?)
- risks (what are the threats and opportunities to achieving this and what are we going to do about it?)

It is not atypical for organisations to have all of the above information in different management systems or documented separately. Bringing it all together through some form of systemic visualisation, however, brings significant clarity to the decision-making process, with the added benefit of gaining crucial buy-in to the risk process through better understanding of the interconnectivity of the respective elements.

Putting it into action

I have first-hand experience of the benefits of this approach, having designed and implemented risk visualisation systems at both Network Rail and Transport for London in the United Kingdom. It included mapping risks to objectives, displaying key performance and risk indicator information, linking risks through causal relationships and highlighting the overall status of controls and progress of management actions. This systemic approach to risk visualisation has proven highly popular with executive committees and boards, having stimulated numerous interesting discussions and prompted several key decisions.

These high levels of engagement from executive committee members should come as no surprise. They are "big picture" people after all! Giving them the tools to visualise their organisation, including their goals and the perils and opportunities they may face in achieving those, has aided their understanding in a way that no risk register ever could. Two other huge benefits of the visualisation approach, if done right, are the interactivity it facilitates and the ability to tailor the information to specific audiences.

Imagine, for example, a CFO wanting to interrogate their organisation's risk information. They may start off looking at all organisational objectives, filter out any non-financial objectives and reveal the strategic threats and opportunities associated with these.

Some threats may be highly interconnected with others and have a suboptimal set of controls, indicating a potential single point of failure. Drilling into these may reveal details about performance dropping off, key risk indicators trending negatively and mitigating actions that are non-existent or behind schedule. This can clearly stimulate some frank discussions and much-needed decision-making about resource allocation and prioritisation of efforts.

Risk visualisation facilitates this on-demand customisable view of what matters to different audiences and enables drilling down with pinpoint accuracy into the key areas that require attention

Figure 1: Executive directors are highly focused on outcomes. This visualisation depicts organisational objectives at risk, and how certain uncertainties (eg supply chain disruption) can affect multiple objectives. These threats or opportunities should typically be addressed as a priority to maximise effectiveness

Figure 2: Highly interconnected risks may indicate single points of failure or vulnerabilities in the organisation. Highly interconnected risks with exposures outside of corporate tolerances that are poorly controlled may indicate areas for urgent attention.

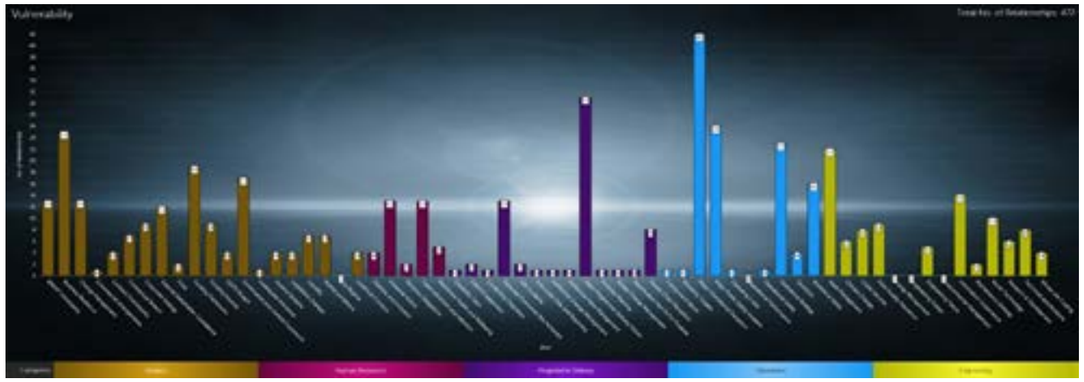
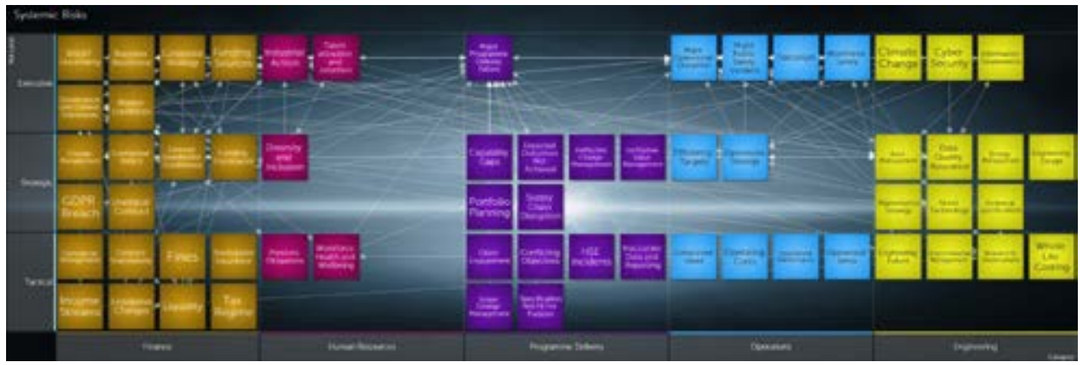


Figure 3: This visualisation depicts risks at executive, strategic and tactical levels in different departments of a fictional organisation. It also shows how risks are interconnected across departments, and how a systemic approach to addressing risk is more appropriate than a siloed approach.



Implementing a risk visualisation approach

Organisations have vastly different approaches to risk and performance management, with data potentially spread across a number of disparate data sources. This makes a one-size-fits-all approach very difficult, if not impossible. I prefer to take a principled approach to risk visualisation, the principle being that you start from what you have and evolve the system to enable the kinds of decisions you want your decision-makers to be able to make.

To start, map out the types (eg risk, performance) and location (eg cloud, on-premises SQL Server database) of information that you need to bring together to enable better decision-making. Next, list the data types (eg numeric, text, list) of relevant information contained in each of these data sources. You can then start dreaming up the kinds of visualisations you want to see by drawing up examples of how these data elements combine to create effective visualisations. Finally, you can configure a visualisation tool like Sharpcloud to access and display the different data sets exactly as you designed it on paper. In addition it even offers a completely interactive 3D view of the risk universe as depicted in the figures on the next page (one with no filter and one with high-risk view).

Specific benefits of this approach

There are many benefits to a systemic risk visualisation approach, some that I am even yet to discover!

- Seeing a network map of enterprise-wide risks helps the viewer to appreciate the risk landscape in its entirety as opposed to having tunnel vision of the risks only affecting one department. This usually sparks entirely different and more strategic conversations.

Figure 4:

3D Visualisation of risks

Figure 5:

3D Visualisation of risks with high impact

- Highly interconnected risks may expose areas of significant vulnerability or single points of failure which may have wide-ranging repercussions should they materialise.
- Risks above corporate tolerance at any level of the organisation become highly visible, which could support decisions around risk mitigation prioritisation.
- The combination of highly interconnected, poorly controlled risks above corporate risk exposure tolerances with an imminent exposure, outside of key risk indicator thresholds and linked to key strategic objectives, may highlight areas for immediate attention!
- Enterprise-wide opportunity prioritisation is easier to accomplish.
- The aggregation and simplification of a complex data set makes it easier to understand and digest.
- The ability to drill up or down to any level of detail and to filter only required information makes risk visualisation the perfect tool to tailor risk conversations to any audience's needs. This increases interest and engagement in the process of supporting risk-based decisions.

Drawbacks of risk visualisation

The main drawback of risk visualisation is generic to any information-based decision-making tool: the information you visualise is only as good as the inputs that go into it. Visualising your organisation's risk information will only serve to highlight any gaps or inaccuracies in the underlying data set and could undermine confidence in the risk process. It is therefore crucial to get assurances that the information is timely and correct before revealing it to any audiences.

Other drawbacks include that the abstraction of risk information could oversimplify nuanced information, which could lead to incorrect assumptions and poor decisions. Furthermore, a poor risk visualisation design which doesn't include the right type of information and doesn't take stakeholder requirements or the types of decisions needed to be taken into account could lead to a lot of effort with very little benefit to the organisation in terms of improved risk-based decision-making.

The ultimate goal

I foresee the ultimate goal in terms of risk visualisation as an integrated approach where real-time information from multiple data sources including performance, risk, assurance and project information is automatically collated, aggregated, updated and presented on demand to decision-makers. This would remove any inaccuracies introduced through manual handling of the information but could result in the information changing while presenting it to an audience.

A functionally limited and static version of this is possible by creating a dashboard using business intelligence tools like Power BI, Tableau or Qlikview. A much more dynamic and interactive version of this is possible through visualisation tools like Sharpcloud; however, in some cases the integration piece may require some investment in developing software linking the disparate data sources to the visualisation software through an application programming interface (API).

I think we are on the cusp of a revolution regarding the recognition of the value and power of an integrated, systemic and embedded risk-based decision-making approach. Risk visualisation could well be the means of bringing all the required ingredients together making the right information accessible to decision-makers at all levels of organisations.

Risk culture building

Horst Simon

The Risk Culture Builder

Regulations, cyberattacks, security situations and global climate change – paranoia in a world that is still just a spinning ball with an increasing population, a place where businesses seem to boom today and are gone or "acquired" by tomorrow evening. This is the world of disruption in which risk managers must advise and support business managers to survive and build competitive advantage over peers and over future competitors that do not even exist in the marketplace today.

To top all of this, we have seen the toxic culture of corporate greed and deceit spread from banking into auto-making and lately to pharmaceuticals. Rigging is no longer a term associated with physical hard work, and scheming (an adjective that describes someone who is always doing sneaky things to make things happen) is now evident in corporate boardrooms. It is almost a world in which bribery and corruption are perceived to not be criminal activities, but gladly still a perception that changes very quickly when you are caught. "White-collar crime" is too often resolved by the payment of large fines without admission or denial of any wrongdoing.

Chief risk officers and risk managers are often wrongly seen as super humans who can single-handedly own and be responsible for the identification, reporting and mitigation of all risks inside and outside the business. How did we get all of this so wrong, and how will we fix it?

"Risk culture is the balance of people, controls & chaos at the edge of business performance" was a quote from the weekly Risk Culture Builder quotes, and reaction to this went as far as a comment saying: "Risk is not part of culture", so with all the perceptions and opinions out there, let us look at getting some clarity from this chaos.

Change starts at the top. Executives live in a space of information overload, and risk reporting sadly fell into the same trap. Board risk reports in many organisations produce more information than what can be digested and certainly much more than what is needed to make better decisions. The first step is to filter this to what is really required and useful, so many risk reports are just presentations of historical "data" that is not converted into "information" and thus not of much use to those whom it is presented to. The risk visualisation article in this publication is one way to move away from this information overload.

Filtering brings us to three key elements to watch, *money, risk and change*. Money is why we take risk as the essence of any business is to take risk for reward, so we have to watch the money; bad cash flow kills companies, and as we see more and more now, so does greed. Find that balance between risk and reward, and always remember that you can only take more risk as you get better at risk management; thus more money is a result of better risk management, nothing else. Those who still see risk management as preventing things from going wrong will differ with me here; those who understand that risk management is about management of risk and opportunity will understand and agree.

Secondly, you must watch the risk, both the levels of risk internally and externally, as well as emerging risks, including those that do not presently exist. There are two big pitfalls here: trying to identify all the risks and focusing more effort on the internal ones rather that what is outside of the business. You can never identify all the risks you are exposed to, so the ability to assess risk and take the best decision in response to that situation of risk is more important than risk identification. The basic risk management process should start with managing the ones you know about and consider to be above the current acceptable levels within your risk appetite. So many executive teams struggle through pages and pages of risk reporting on what is internal to the business and focus all the risk management efforts on controlling everything internal to the business; this is similar to building a bomb shelter, but not putting sandbags on the outside - a pretty useless exercise. Generally, what is inside is well known, and if you are still in business, reasonably well managed; the ones from outside are the ones that are most likely to put you out of business. Too often, I hear and see executive teams trying to drive the profits up and the risk profile down; getting all the risks "green" will never bring sustainable growth and certainly not bigger profits.

The third key element after filtering the information overload is change. The world is changing at an unprecedented pace; the levels of change are much bigger than before, and change is happening much faster than before. During any phase of change the level of risk increases and new risks are introduced during the process, or sometimes because of the process. No business can exist without human intervention, and there is a limit to the level of change and the pace at which any human can accept such disruption. So often, we see examples from the oil industry where they launch a multitude of

new projects, restructure, enter new markets, change operating systems or involve themselves in mergers and acquisitions, all at the same time.

The foundation for success must be built at the top, and from that level down the strategy must be clear on the goals for money, risk and change, in a balanced way.

How much do we need to make? How much risk will we take to do that and what if things go better or worse? How much change can we afford and cope with? "Make as much as we can" is not a goal; it is a recipe for disaster.

Once the foundation is laid, we can move on to the future of risk management. The most difficult change is to move on from risk management being seen as an obstruction to business that is only relevant in industries where there are regulatory requirements to be complied with to the understanding that it is essential to drive value and sustainability. Risk management operations in any business must deliver a positive return on investment. Risk management is not part of the cost of doing business; it is the driver for business success.

However, there is always the risk of employees seeking to maximise their bonuses who may take excessive risks, particularly if their bonuses or other incentives are based on immediate results and ignore long-term profitability and prudent risk management. In the oil industry there are numerous examples of major accidents occurring due to cutting corners in order to meet schedules, or risk management being silenced in order to hide true completion dates in order to achieve quarterly bonuses.

The second challenge is changing risk reporting from this rear-view mirror picture based on historical, often inaccurate, data to something that is forward-looking and can support better decision-making in the business. Even with more than 16 years of experience in operational risk, I still cannot understand the importance and focus placed on historical risk reporting and often ask the question: "Do you care about how much fuel was in your car last week?"

Risk management through people

Building an effective risk culture is much more than changing your organisational culture in line with your vision, mission, corporate values and risk appetite – you must factor in the interests of competing national cultures, sub-cultures, Maslow's theory on hierarchical needs of individual self- actualisation and the informal groups in the company. The interactions between these are not predictable and variables cannot accurately be isolated.

An effective risk culture is not a matter of risk assessment or level of compliance; it is a matter of "conviction" – a corporate state of mind where human beings can take well-informed risk decisions because they want to, not because they have to. Risk policies, systems and reporting dashboards are all part of the foundation for good risk management. Once you have these in place, you can start building an effective risk culture. Remember also that there is too much complexity and subjectivity in culture to assume that individual reactions and responses can be aggregated to reflect or give an accurate picture of the whole organisation's risk culture. You cannot "pop" an effective risk culture in the microwave; it takes a lot of preparation, dedication and time to get it to perfection.

The future of risk management is not just looking at the windshield. Scanning the horizon might just be the most important thing to do. You cannot control or stop what is coming; you must prepare to respond to it. So many organisations spend large amounts of money to focus and report only on what is happening inside the organisation, where they have control. Your biggest risks are outside of the organisation, where you have no control.

Key elements for the future of your risk strategy should include internal networking; you must talk to the informal groups and their informal leaders just as much as you do talk to the executives and managers, maybe even more. The real business is not always done in the formal "boxes and lines" structure.

Just as important are the aspects of desk research and external networking. To have a good risk management strategy and action plan, you should know everything about your industry, markets, competitors, supply chain, alternative supply chain, global risks in an interconnected world and many more. Failure to adapt your business model, which drives your "risk for reward" system, to the ever-changing internal and external risk environments will lead straight to the corporate graveyard.

The future of risk management is just "risk management through people". You can have the best systems, great models and scenario analysis with elaborate dashboards; at the end of the day a person will take a decision.

Are your employees aiming at more than one target, or do you have a clearly defined risk for reward strategy and risk appetite statement to guide them? Business strategy and risk culture are parts of an interdependent system.

Start working on your success by training every employee so that they gain some basic risk management skills.

To quote Sarah Tennyson: "Enterprise-wide risk management requires a shift in the behaviour and mindset of employees across an organisation. To realise the full benefits of improved systems, tools and analytical skills, people need to learn new ways of perceiving situations, interpreting data, making decisions, influencing, and negotiating".

Getting used to the transparency of a risk management framework is the first stepping-stone in building an effective risk culture. Within the context of having a risk profile, learning to not focus on the risk, rather the optimisation of it, is the next step.

Having an accurate risk profile for each business area and a consolidated picture of the main risks creates a valuable opportunity to reconnect with your business, build trust among your people, will improve decision-making and provide transparency to your stakeholders.

Being risk aware rather risk averse will show commitment in diligent business practices and allow the business to grow through the commitment of every employee.

A more effective approach to risk appetite

Alexander Larsen CFIRM, IRM Energy SIG Chair
and Ghislain Giroux Dufort MIRM
Baldwin Global

Establishing risk appetite and tolerance levels (and monitoring over time the actual risk profile against them) is essential to the long-term success of any organisation, whether in the energy industry or other sector of activity.

When discussing risk appetite, people tend to think of bland and non-informative risk appetite statements, or overly quantified and financial risk appetites. Both of these have limited value. Looking at the high-level risk appetite statements, they are nearly always:

A) Too broad to gain any significant use out of the statement

- How can decisions realistically be made from a statement such as we "will not accept any risk that affects our reputation"?

B) Rehashes of the corporate objectives or taken from other targets such as HSE accident rates

- An organisation could have endless risk appetite statements that would allow no risks to be taken if this was the case.

C) Inconsistent with objectives

- How can an energy company operate in an environment where a risk appetite statement says "we will not accept project delays of x" or "we will not accept loss of life." The nature of the business is projects and delays, while operating in countries such as Iraq or Afghanistan goes against "we will not accept loss of life". The statements are too broad and lack detail or real decision-making value.

D) Never change

- Once an organisation sets a risk appetite statement, they rarely change, and why would they? It's a very high-level statement that can only be written in a small number of ways.

E) Don't consider the risks

- The risk appetite statements we have seen are almost exclusively linked to objectives, which doesn't take into account the actual risks that the organisation faces.

Most organisations struggle with putting together even the high-level type of risk appetite statements. They often spend a lot of time and resources on trying to perfect high-level statements that don't provide much decision-making value, or on overcomplicating the statements, which again leads risk appetite to being ineffective.

In this article we highlight a methodology that provides decision-making value to quantified risk appetite statements by linking corporate objectives to leading KRIs established at the source of risks that may affect the achievement of those objectives. This approach provides a warning system that increases the chance that organisations may take action before risks materialize.

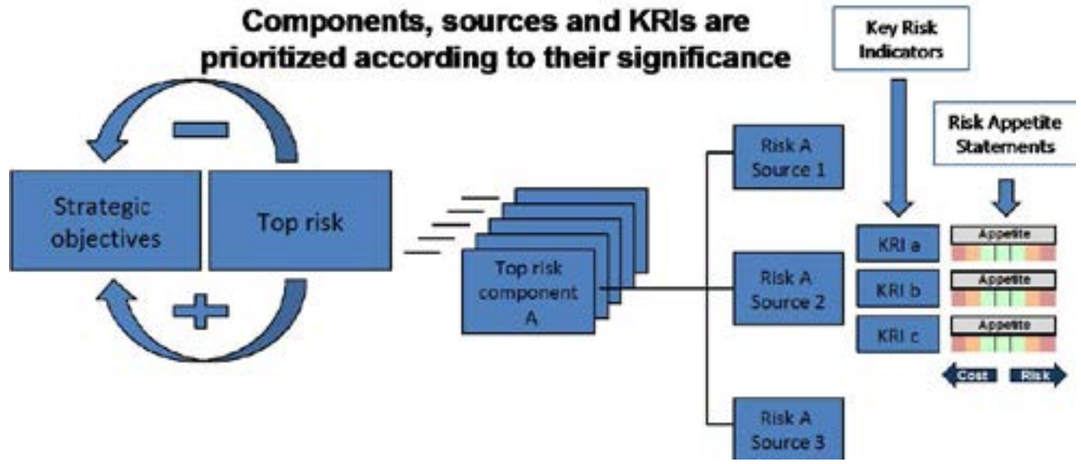
Objectives v risk

While the whole point of risk management is to identify and manage risks to the objectives, risk appetite statements tend to focus solely on objectives, for example aspirations of zero accidents or deaths. Risk appetite therefore ends up driving risk identification rather than the risks driving the risk appetite.

Assume an organisation has 5 key objectives, and 5 major risks. Once targets and acceptable deviations relative to targets have been set for key objectives, how does the organisation manage to minimize the chances of deviating from key objectives? The answer is to focus on the major risks to key objectives and to set risk appetite statements for these risks rather than only on objectives. Assuming that risks change more often than objectives, we can also expect the appetite statements to change more frequently too.

One other major benefit of linking appetite to risk is that we can actually map the risk through to the relevant key risk indicators (KRIs) with individual risk appetite ranges for each KRI as shown in Figure 1 overleaf.

Figure 1: Baldwin Global's Key Risk Indicator and Risk Appetite Model



How to set risk appetite and key risk indicators in your organisation

In our experience, high-level risk appetite statements based on each major risk can be put together in a half-day workshop with management teams. Detailed quantified risk appetite statements based on KRIs established at the source of risks will require some more time depending on the nature of the risk and availability of data and expert opinion. It is important to run workshops rather than setting these statements in isolation. Not only does it ensure everyone is aware of the risk appetites, but there is the added benefit of increasing risk knowledge and building a positive risk culture while also gaining a variety of views and experiences to develop the appetite statements.

Of course, when setting statements, it is important to consider the wider implications for the organisation. Rather than setting a figure for what is acceptable in terms of accidents or deaths for example, AirSafeCo, the fictitious airline company example below in Figure 2, decided to look at improvements to long term trends and focus on not accepting an increase in the trend. This presents a more sensitive approach to safety risk and its management over time, rather than having an "acceptable" number of casualties or fatalities.

In addition to the general risk appetite statement written in Figure 2, more specific and quantified statements should be established based on leading key risk indicators linked as closely as possible to the source of the risk. Figure 3 illustrates such a statement for AirSafeCo's three top components of Safety Risk: Crash, Turbulence and Tarmac delays.

Figure 2: AirSafeCo's General Risk Appetite Statement

Risk	Definition	Strategic objectives potentially affected	Impact categories	General risk appetite statement
Safety	The safety of passengers may be negatively impacted by a crash, turbulence, delay on the tarmac or other events	• Be the safest airline company in the world • Have the highest customer satisfaction of the industry	• Health and safety • Financial • Reputation	AirSafeCo has no appetite for an increase relative to the 5-year historical average in the number of annual safety incidents. AirSafeCo seeks to reduce the probability of occurrence and the potential impact of such events and to be prepared to recover compassionately and timely should such an event occur.

Figure 3: Examples of KRIs and how to build a risk appetite linked to them.

Higher cost → Higher risk

	Risk tolerance		Risk appetite			Risk tolerance		
	RED zone	ORANGE zone	GREEN zone			ORANGE zone	RED zone	
			Lower limit	Historical or target value	Higher limit			
Safety risk								**Key Risk Indicators**
	Number of accidents							
General risk appetite statement	AirSafeCo has no appetite for an increase relative to the 5-year historical average in the number of annual safety incidents. AirSafeCo seeks to reduce the probability of occurrence and the potential impact of such events and to be prepared to recover compassionately and timely should such an event occur.							**Tracked quarterly**
Crash	NA	NA	y	x	z	range	range	Near miss
Turbulence	NA	NA	y	x	z	range	range	Time to buckle up
Tarmac delay	range	range	y	x	z	range	range	Air control/ airport data composite

The Green Zone represents the quantified risk appetite for each risk component: the amount of risk the company is willing to accept in order to achieve its objectives. The Orange Zone represents the first level of tolerance and may require, for example, an investigation into the reasons for this deviation. The Red Zone represents the highest level of tolerance where immediate action is required. More risk tolerance zones may be inserted to provide various levels of analysis and/or action. Leading KRIs of crashes might be, for example, near miss events. In turn, one could then search for leading indicators of near miss events, and so on. Each industry and company should find or create leading KRIs that are causally correlated to their key risks and linked to their impact on corporate objectives.

Risk workshops may provide expert opinion on KRIs and appetite and tolerance levels. But having the right data to validate those opinions is essential too, and it is therefore important to understand what the components and causes of risks are, in order to understand what information is required. As an example, for an oil & gas facility in a sensitive area, the risk of "major loss of life" could come from a terrorist attack, major accident or natural disaster. Once you have identified the components and causes of major risks, KRIs can be established which allow individual risk appetites set at their source.

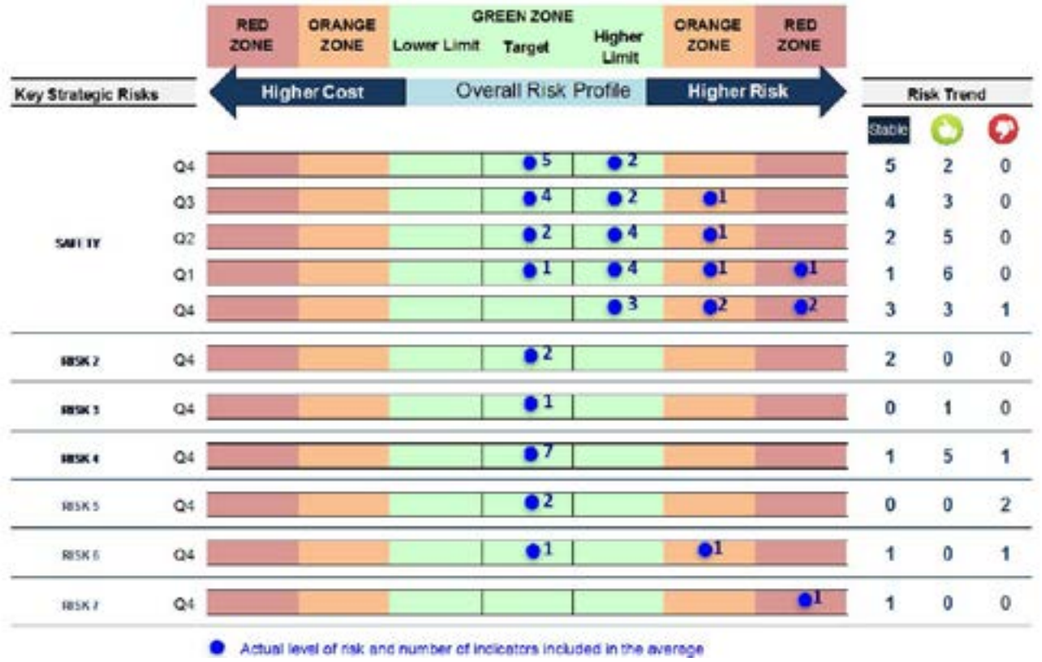
Also note that Figure 3 is two-sided: the right side indicates positions of increasing risks, while the left side indicates positions of reducing risks - but at an increasing cost. Since risk management is not free, trade-offs may have to be made when deciding on risk appetite and tolerance, and the cost of managing a risk to its appetite and tolerance can also be monitored using this approach.

How does this help decision-making and risk reporting?

One of the roles of risk management is to enable boards of directors and senior management to make better strategic decisions. Too often, organisations limit themselves to reporting risks independently, through risk registers and heat maps. This is very limiting and often out of date. Additionally, risks rarely change significantly which means the top 3 or 4 risks (in terms of likelihood and impact) are discussed at length whilst the others get missed. What should be done is to integrate risk assessment and reporting within business cases for decision making purposes.

As we have seen earlier, risk visualisation is a far more effective method of viewing risks for decision-makers, offering an alternative view of what the top risks might be. The approach to risk appetite and KRIs that we have

Figure 4: Example of Risk Reporting based on Appetite



so far discussed offers yet another alternative to the traditional risk register approach to reporting. It provides real-time snapshots of the status of risks to the business and a perspective on their trends. The top three to four risks on most risk registers are usually very well managed, and senior management would be better off discussing the other risks that might be less well managed. A visually effective reporting template allows for such focus on relevant risks and is demonstrated in Figure 4 above.

Looking at the reporting example in Figure 4, the output from the KRIs and the related risk appetites shows clearly which risks are most pressing. Senior Management and the Board would be able to tell quickly which risks are within their appetite and which ones lie outside their appetite or tolerance levels. A focus on the last five quarters of Safety risk shows that KRIs have gradually improved over time towards the Green Zone, a sign that enhanced safety risk management has paid off in this example.

Conclusion

Whether they operate in the field of transportation, energy, or any other sector, including not-for-profit ones, organisations need to take risks in order to achieve their objectives and to thrive. Where risk appetites and tolerances have already been determined, it is counterproductive to be over-managing risks. One of the unique aspects of this approach to risk management and reporting, aside from focusing on risks that really need attention, is that it also exposes risks which may have too many controls and where resources would be better spent elsewhere.

A more effective approach to reputation risk management

Hans Læssøe

Principal at AKTUS

Reputation risk considerations

The term "reputation risk" is heard more and more frequently and the increasing use of social media exacerbate the importance for any organisation to have a deliberate stand on its reputation and ensure this is being managed. The below constitutes a description of the concept of reputation risk as well as some thoughts related to possible actions and safeguards that can be prudently taken.

First and foremost, reputational risk is not "one risk', but rather a category of risks, which may impact your reputation. You do not wake up one morning and have a bad reputation - something happened prior to that to generate the bad reputation. The real risk emerges from "what happens".

Furthermore, it is important to note that the incidents invoking reputational demise may not be of your own doing or influence, which is amongst the reasons the term gets the attention it gets at present.

As shown in Figure 1, reputation risks may be of your doing and hence within your control.

Figure 1: Reputation risk

Others		
Yourself		
Who/what	Did something and should not have....	Did not do something and should have...

However, it may also be an outcome of actions made by others, and hence outside your immediate control. Such third party actions may be made to intentionally harm your brand and company - or they may be made without any consideration as to any impact it may have on your brand and company. Thr fact that you cannot control third party actions does not mean that risks cannot be mitigated.

Naturally, the company/organisation itself is the prime driver of sources of reputational risk. Any diversion from the safe and prudent, well managed and honest leadership map invoke reputational risk. Much of the above is in this category.

Logically, behaving badly drives a poor reputation. The most impactful of these is being in breach of laws and defined regulations, especially if/when it is at the expense of the "little guy", e.g., the shop floor work. Health and safety violations create a bad reputation fast.

Unethical behaviour, e.g., exploitive child labour in Asia, is also seen as bad behaviour and will have a negative impact on your reputation - even if/when this is being done with the best care and respect for the children.

If/when what you deliver is not safe in use or foreseeable misuse, your reputation will be at risk. Product safety requirements must be adhered to, to safeguard your reputation. Note here that, for example Smith & Wesson making guns or Benson & Hedges making tobacco products do not have a bad reputation based on their product, whereas a toy leading to the death of a child is devastating, as was the case with the Magnetix toy from MEGA Brands.

Products can be used for other purposes than intended, and when this happens the reputation of the manufacturer becomes at risk. The Danish pharmaceutical company Lundbeck manufactures a sedative which is being used as part of the "lethal injection" process in US prisons. This was not intended, nor "approved" by Lundbeck - but as it is happening, Lundbeck is the pharmaceutical manufacturer that kills people.

Arrogance or insensitivity in communications and/or actions also deplete a reputatonal risk. For example, when BP experienced the Deepwater Horizon accident, they first accepted full responsibility and promised full recovery. The attitude towards BP was not bad - given the severity of the situation. However, when it later became clear that they lied about actual issues, and the accident was a consequence of a consistent cost cutting focus the "hammer" of bad reputation hit. When the CEO added insult to injury by stating that "I want my life back", the reputation of BP hit an all-time low.

In many countries, there is a positive perception of companies that "do well" and are highly profitable.

One prominent example is Apple's Steve Jobs, who was not the ideal executive and people-leader in many respects, but because it was under his reign that Apple became so enormously successful, he was seen as a hero. If performance drops, yesterday's hero becomes today's "villain" - also seen in industry. Enron was highly commended in business and press and everywhere - until the day the bubble burst, and then...

You know this from buying a car. If you buy an expensive car, and you experience some fault, you initially get angry/frustrated as that "should not happen" with an expensive quality car. However, if your claim is handled professionally, expediently and supportively, you may very well end up thinking "*I'm glad I bought this brand because see what service I got*". You may at the same time own a car from a less prominent brand with which you do not experience any faults - yet, that brand is still accepted. Reputation can be built, even on mishaps.

Reputation risks may also be forced upon your organisation from outside the company - not directly related to what you are doing.

A case example: Originally, the French wine industry had a huge share of European wine consumption. Then the French government decided to test nuclear weapons on atolls in the Pacific - despite public outrage. This lead consumers, especially outside France, to "boycott" French wine and buying products from the US, Chile, Australia, Spain, etc. French wine has never regained their market share.

In Denmark, a newspaper decided to run an article on self-censorship towards religion. To make a point, they asked a series of cartoonists to make a drawing of Mohammed. Few did, and the drawings were published with the article. During the first several months, nothing happened, but then a team of people reignited the issue by contracting Muslim societies and dignitaries to create an outrage. This was quite effective, and led to several Arab countries banning Danish-branded products. These brands had nothing to do with the cartoonists' drawings of Mohammed, and they still experienced a severe drop in reputation and sales.

Sources may even be hostile attacks on your reputation. This is no more visibly seen than in a US presidential race where "negative commercials" are a significant share of the campaigns launched. In later years, this has been exacerbated by use of "fake news" appearing to be third party and indirect communications, which impact the stand of the opponent.

In history, governments have survived based on limiting and controlling the information given to the people. Some still apply this approach. Today, the Internet, social media and SMS chains break down these barriers - first seen with the public upraise that eventually led to the fall of the Berlin wall in 1989, later seen in the Arabian Spring.

Facebook fan groups are established and gain membership in millions over weeks or even days. Twitter users scan the world in minutes - so if you are operating globally, an incident can lead to global pressure between the time you recognise the issue and the time you have assembled your crisis team.

Handling speed requires preparation, and one important mitigation is knowing who will address any issue - and make very sure these people can team up very fast, and any time 24/7/365 if need be. This calls for explicit and well prepared reputational risk management.

Business impact may emerge suddenly and may vanish fast, but will most often be rather slowly. Dents in your reputation tend to be remembered, highly depending on your defined image/reputation and industry. The loss of credibility will often have an immediate effect on your stock value as stock brokers race to embed new insights first, and hence act on everything and anything they learn, now (even if/when what they learn has no short-term consequences). Losing stock value hampers the company's manoeuvrability and hence long-term prosperity.

Your sales may be impacted by customer actions "banning" your products. This will naturally lead to loss of profits as well. Your collaboration with vendors and partners can be hampered, and you will be met with increasing demands of documentation and other issues of "red tape" based on reduced trust on behalf of your partners. You stand to lose employees, who will not work for a company that "does this or that" - and it will be the best people who will resign from the company first, leaving you with a "B" team.

Having a strong and positive reputation is a strength, but it also increases the impact of loss. Your reputation has to be safeguarded.

As mentioned, when faced with an incident that negatively impacts your reputation, you must be able to act fast, effectively and "right". You also need to have some metric of what is "high" impact on reputational risk as you will be acting too late if you measure in the annual

report. Such scaling is a core competence for experienced risk managers - and by the end of the day, a managerial choice of risk tolerance.

Having a pre-defined team, with pre-defined reference frames and full authority to act is pivotal to good handling of reputational risk. In some instances, a response must be visible world-wide within hours. Some companies even excel at acting so fast and effectively that hiring them is good for your reputation. It is highly recommended to form task forces, and to have them conduct “fire drills” every now and then to ensure efficiency.

It is also recommended to imagine a set of risk scenarios - and discuss these prior to their potential emergence.

Soldiers do this all the time, on safety. All routine tasks are rehearsed and rehearsed to the almost ridiculous - to ensure that, in the midst of a crisis doing these routine tasks does not occupy attention, which can then be directed towards dodging incoming fire. This approach can be applied by companies for reputation risks as well.

Finally, there are naturally the pre-emptive probability reduction efforts of behaviour. Do good for the community, be open and honest and drive a stable and profitable business.

Having your reputation “at heart” and remembering this when deciding on strategies and business initiatives is well worth the effort - and may even serve to safeguard your profitability more than a mere commercial focus.

Conclusion

While the energy sector is embarking on a period of expansion involving new initiatives, territories and energy sources, the risk management expertise required to make that an effective transition is only partly in place. Having risk management “established” in many companies, may not be enough to enable risk professionals to place risk at the centre of strategic and operational decision-making.

Risk managers have highlighted several barriers to their effectiveness – budget and resource constraints, occasional failures at board level to set the right tone on risk and a relatively low take-up of specialist ERM software to enable the implementation of cutting-edge risk management across globally distributed organisations.

On the other hand, risk managers are involved in a wide range of areas across their businesses – from project risk to supply chains and security.

In addition, many are reporting to the board more regularly than expected and supporting management with frequent risk reports. Building a robust risk culture is becoming a key focal point for many energy companies.

We hope that the insights contained in both the survey results and the in-depth articles we commissioned for this report will help spread best practice among professionals working in the sector. We are, after all, a community of risk managers working to help our organisations make better decisions. The report authors would urge members to get involved in the activities of our Special Interest Group (SIG) so that we can continue to strive towards that aim.

For more information about joining the SIG, please email: **marketing@theirm.org**

or visit: **www.theirm.org/energy**

Institute of Risk Management
2nd Floor, Sackville House
143–149 Fenchurch Street
London
EC3M 6BN

Developing risk professionals