EMERGING TRENDS IN RISK MANAGEMENT
Kogan Page is the leading independent global publisher of specialist content, from books and supporting resources to toolkits and case study libraries. Kogan Page publishes books on business and management skills, international business, information and data management, leadership, management science, risk, strategy, compliance and regulation and corporate governance. Our author experts are members of the most prestigious academic institutions, international commercial organizations and professional associations.

The following are the most popular articles and extracts by Kogan Page Business, Leadership, Risk and Information Management. Written by our author experts, they both address current issues in and point to the exciting future of management, business and leadership.

CONTENTS:
3 Legal Risk is a Big Worry for Large Businesses by Matthew Whalley
4 How Do Risk and Change Fit Together? by Ruth Murray-Webster
5 Behavioural Risk: The New Regulatory Challenge by Dr Roger Miles
7 Acknowledging Risks from The Cyber Lucifer Effect by Ben Rendle
9 Rethinking Reputational Risk by Anthony Fitzsimmons
10 How to Design Your Own Risk Maturity Model by Domenic Antonucci
12 Achieving Corporate Goals and Resilience through Risk Management by Edward Sankey
13 What’s Your Appetite for Risk? By Paul Hopkin
14 A Case of Two Managers: Different Approaches to Managing People Risk by Keith Blacker
15 What Is Risk Culture and Why Should We Care About It? by Alex Hindson
Legal Risk is a Big Worry for Large Businesses

By Matthew Whalley

Legal risk is a niche risk area that is about to enter the mainstream. Previously the sole responsibility of in-house lawyers, changes to risk governance and corporate governance are putting legal risk in the spotlight. Businesses need to step up and decide who will own the second-line responsibility for legal risk identification and reporting, who will own the losses associated with legal risk, how those losses will be recorded, and who will give assurance that legal risk is being managed with due competence.

Individual accountability at board level has put the spotlight on legal risk reporting

Legal risk and corporate governance are inextricably linked. No sane CEO would set out a business strategy that could result in huge losses and possible criminal sanction. And no sensible board would rubber stamp decisions that could potentially ruin their business. But the corporate governance structures that boards put in place to ensure their decisions are implemented have come under increasing scrutiny since the financial crisis. There is a rising tide of regulatory reform aimed, in part, to strengthen corporate accountability that demands prudent institutions re-assess the effectiveness of their existing corporate governance structures - and their approach to legal risk. Firms are increasingly being required to evidence how corporate governance principles are applied not just at board level, but throughout your organisation wherever management decisions are made. And this requirement maps to new expectations that boards will have a clear view of the actions that staff at the front line of their business take and their effect on the legal risk profile of the company.

The decisions you take in the boardroom set the parameters within which legal risk is managed within your organisation. Corporate governance failures were at least partly to blame for banking failures in the financial crisis, in particular where boards were dominated by powerful individuals whose decisions weren’t subject to robust challenge. Much of the new thinking around corporate governance centres around the make-up of the board, and how to ensure that decisions of CEOs in particular are subject to necessary checks and balances. But boards also need to be certain that corporate governance delivers the right behaviours and outcomes throughout their company. If boards and senior management don’t take seriously their responsibility to oversee the culture and behaviour of people in your business, legal losses are almost certain to follow. And senior executives are at risk of criminal sanction if their organisation suffers a severe failure in corporate governance.

This individual accountability has forced boards to take an active interest in how the policy and values they set at board-level are interpreted into action throughout their business. And this ties in with new approaches to legal risk management that are designed to provide evidence that corporations’ working practices are in line with their stated values, and don’t expose them unnecessarily to legal risk. Legal risk management produces data that speaks not just to the internal reference point of your corporate value statement and policy framework, but also to the external reference points of law and regulation.

Adapt your Operational Risk Frameworks to Incorporate Legal Risks

Legal risk is aligned to operational risk. Operational risk frameworks can be adapted to capture legal risks and encourage in-house legal teams to identify and quantify legal risks and articulate the root cause of the risk in a way that is meaningful to operational risk teams and front-line business colleagues. To bring legal risk to life for your business, analyse the
potential impact in direct financial and indirect (non-financial) terms. Impact analyses are used to evaluate legal risk across the enterprise, and to model and prioritise legal risks against other enterprise risks.

The practicalities of legal risk identification cut across a wide gamut of legal disciplines and business areas. In our new book, we talk not just about how to align legal risk management with operational risk and corporate governance, but we have captured best practice in how to manage the risks within five categories of legal risk: legislative/regulatory risk, non-contractual obligations (duty of care) risk, contractual risk, dispute risk and non-contractual rights (IP) risk. We hope that our book will help guide in-house legal teams’ efforts to identify legal risk, prioritise and report them, and implement best practice legal risk management and controls throughout your organisation.

HOW DO RISK AND CHANGE FIT TOGETHER?

RUTH MURRAY-WEBSTER

Ruth Murray-Webster, the author of chapter 18 in The Risk Management Handbook on organizational change management and risk argues that (i) all organizational change is risky and (ii) most organizations need to change some things in order to get the benefits from risk analysis and management.

Before unpicking these statements a little, it is interesting that discussions about organizational change in professional bodies, academia and practice often focus on the binary notions of ‘success’ or ‘failure’.

The Association for Project Management has a vision for a ‘world in which all projects succeed’. Many learned books and consultants start any conversation about change by stating the popular myth that ‘70% of all change initiatives fail’. It seems to Dr Murray-Webster that these binary discussions miss the point. Most organizational changes are at the same time wildly successful and spectacularly disappointing, and everything in between, depending on the point of view of the stakeholders involved. We only have to look at the organizations we are part of (at work, church, football club) or to read newspapers to know this is the case – it’s a sad truth that we rarely please all of the people, all of the time.

In all cases, organizational level objectives for change require people to change the way they do things – use different processes, different systems or to behave in a different way. The research underpinning this chapter highlights the fact that people do not change the way they perform tasks unless their internal thoughts, feelings and intentions for the work first change. Many change initiatives focus on macro level plans, but do not focus on the people with the power to make the change fly, or sink without trace. Understanding stakeholders, particularly those who are the recipients of change, those whose work is intended to change is vital.

Nobody tends to argue with this point, but it is surprising that often the link between stakeholder engagement and risk analysis and management is not made.

In The Risk Management Handbook, the chapter on managing stakeholder risks makes the case for having a really good understanding of stakeholder perceptions and the risks associated with these. This chapter highlights tried and tested ways of analyzing stakeholders and predicting how they might behave in different circumstances.

Such methods are really important in organizational change management but the argument made by Dr Murray-Webster is that the need for understanding stakeholder points of view about change and the need to understand perceptions of risk to change
objectives are so related that we should manage them together. Why have a ‘stakeholder analysis’ process that does not share objectives with the ‘risk identification’ process? Every conversation with a stakeholder is an opportunity to understand points of view and to uncover current views about risks. Conversation is key to uncovering what people really think and we are much more likely to uncover ‘real’ perceptions of risk from people when we truly engage them as individuals.

There are pitfalls to avoid, however, in this process. Conversations about risk can be tricky because, by definition, risks are potential future events and perceptions are influenced by a myriad of different rational and biased mental processes.

For example, we need to understand perceptions of what is risky and why when we are pulling together the business case for change – deciding how much to invest and when – but the risks may be downplayed or emphasized in early lifecycle depending on whether the stakeholder’s objectives are to get the change approved, or to be accountable for delivering the change over time.

Similarly, we need to understand what might happen to deflect us from plan in order to guide and protect delivery – but the perceptions of the people who are the recipients of change are likely to be very different from the perceptions of the project team who just want to get the change done.

Nevertheless, we avoid these tricky conversations at our peril if we want to deliver organizational change.

The binary notions of ‘success’ or ‘failure’ in organizational change are not very helpful. We would be foolish to ignore evidence of the ‘critical success factors’ for organizational change but these are necessary but not sufficient. We would also be foolish to follow a risk management process during organizational change without recognizing that the best way to understand risk is to really engage the stakeholders with the power to make or break the change effort.

This chapter explores these ideas further and offers practical tips for people who recognize that all change is risky and that they need to change the way they do risk management if it is to add value to change efforts.

BEHAVIOURAL RISK: THE NEW REGULATORY CHALLENGE

ROGER MILES

Governments and regulators around the world have recently been paying close attention to a fast-developing branch of social science research: behavioural economics. This Nobel Prize-winning research field studies patterns of human behaviour, and how these create costs, or other harm or benefits, to others. Whether or not you’d noticed it yet, this new(ish) branch of science has been steadily gaining influence and can now affect how everyone conducts their business: not just in the design of risk controls and regulations but also how organisations set about their marketing, fraud control, and human resource management. There are serious and expensive implications for many aspects of life in organisations; here, we’ll just highlight one aspect.

Behavioural economics in practice includes government programmes to ‘nudge’ better behaviour, fixing a range of social problems which had proved tricky in the past – from preventing obesity to catching up with naughty bankers. Here’s an example of a public policy ‘nudge’ that the US and UK governments have both used successfully:

Governments always found it hard to get citizens to save for retirement; with an ageing population, national treasuries seemed to be facing an unstoppable
MISBEHAVING BIG NAME INDIVIDUALS AND BRANDS

Programmes, and co-ordinated prosecutions against misbehaving big name individuals and brands. If you haven’t yet read up about what all this means for your cashflow, now would be a good time to start.

That sort of initiative sounds good for your future, as well as good for government finances. So everyone’s a winner, right?

Not necessarily; read on.

Behavioural economics has grabbed politicians’ attention because the alchemy of ‘nudging’ promises to fix all kinds of social problems at almost no cost to public finances. From Ministers’ point of view, that’s a big win – a rare patch of sunny upland amid a policy landscape of austerity gloom, zero interest rates, currency collapses, and widespread voter anger. To be able to change benignly (in theory) how the voting public behaves, without taxing them while you do so, is thus something of a politicians’ dream.

In case you hadn’t already noticed, one of the first targets for this new regime of ‘behavioural regulatory intervention’ was the financial services sector, with the launch of a new type of ‘conduct regulator’, the Financial Conduct Authority (FCA), in 2013. After all, noted the politicians, those bankers had rather offered themselves up for a public kicking by demanding taxpayer bail-outs back in 2008. A decade on, we face a steady increase in regulation-led ‘behavioural risk management’, and a widening range of organisations caught in the new regulatory regime.

It’s not just financial firms. If you are an advisor to a financial firm, or indeed any brand with a financial subsidiary business – perhaps you’re a high street brand that happens to provide an own-label credit card – think carefully about this: You are now regulated by an alliance of ‘conduct control’ bodies, including the UK’s financial (FCA), credit Prudential Regulation Authority (PRA) and fair trading Competition and Markets Authority (CMA) regulators, all of whom now design their rules using behavioural economic principles. Conduct regulators are also looking increasingly to form international alliances, with new treaties (‘memoranda of understanding’), staff exchange programmes, and co-ordinated prosecutions against misbehaving big name individuals and brands. If you haven’t yet read up about what all this means for your cashflow, now would be a good time to start.

And behaviour-based risk control is expensive. By the simplest measure, all of the new capital that UK banks recently raised for themselves (2013-16) – that’s over £30 billion – they’ve had to expend on conduct regulatory costs: fines, redress, reorganisation, and so on. All the money that banks might otherwise have lent to businesses, they’ve had to spend on dealing with the new wave of behaviour-based regulation. They’ll also be needing £40bn more for this, 2017-20, said the Bank of England recently.

Whilst some might say banks brought these costs upon themselves, bear in mind that other branches of UK government, and indeed many other regulators around the world, are also starting to adopt behavioural regulation principles; the UK’s competition regulator (CMA) already affects potentially every business in the land. Elsewhere, behavioural regulators as far afield as Australia, Hong Kong, Singapore, South Africa and the USA are busy sharpening their own instruments of conduct enforcement. In the past year, Australia’s regulator (ASIC) has imprisoned more than twenty times as many company directors (per head of population) as the UK, for misconduct offences; other jurisdictions aspire to emulate this startling rate of ‘outcome’. Remember, in a political landscape where institutions are widely mistrusted, this new policy direction is a popular vote-winner.

Additionally, conduct enforcers will now intervene to prosecute the non-event of a corporate control system, not just misconduct within an existing set of risk controls. Straight after an organisation suffers the reputational damage of a failed operational control, the prosecutor may now step with an enforcement notice and even a criminal case. One British bank that recently suffered a hacker-induced systems failure then found itself prosecuted for the misconduct offence of having caused ‘customer detriment’ when the network failed.

Regulated and other impacts of behavioural risk – such as ‘socially engineered’ hack attacks – will only rise, unless we take realistic steps to anticipate and head them off. By recognising that these are new forms of threat, we can adopt new approaches to managing risk. At a detailed level, many staff still feel that they don’t yet know enough about what constitutes misbehaviour under the new rules. At the higher level of risk governance, senior managers need urgently to revive staff’s awareness that they can and should use their own intuition for more reliable early warnings of misbehaviour.
Expect this form of disruption to continue, as conduct prosecution is far too profitable for governments not to want to expand it. For sectors facing this – not just in finance, but increasingly for public-facing organisations of all kinds – everyone involved needs to build a new layer of situational awareness. We will all soon have to know how to ‘work risk-aware’ in daily practice. The basic skills needed can be learned through a simple one-day workshop that transforms staffs’ responsiveness to behavioural risks, provides earlier warnings of trouble, and will over time save a stack of fines for misconduct, not to mention wastage of a misdirected compliance budget.

There is plenty else you can do, of course. Whatever preventive steps you do take, it’s no longer an option to do nothing – unless of course you want to star in tomorrow’s bad news headlines.

Acknowledging Risks from The Cyber Lucifer Effect

In 2015, the UK media reported that cyber hackers infiltrated Ashley Madison, a controversial online dating website for secret extramarital affairs. The website claimed a ‘100% discreet service, with a Trusted Security Award on its homepage’ for up to 37 million people worldwide. According to media reports, the cyber hackers are threatening to release all of the details to client’s partners and close contacts unless Ashley Madison goes offline.

The internet can blur activities between individuals, not-for-profit organisations and businesses. What makes this example interesting is the unique online aspects of clients having an extramarital affair. Firstly, hosting a website service enables companies to commercialise extramarital affairs to a global scale and secondly, clients had ‘the illusion that adultery is somehow different, safer, when conducted online’. Online extra-marital affairs do not even have to involve real people, as the UK’s Daily Telegraph reports a case where a woman divorced her husband for having a ‘virtual’ affair with an imaginary, animated woman on a computer game called ‘Second Life’. However, extramarital affairs aren’t the only cases where specific online activity has been the downfall of individuals, not for profit organisations and businesses. Some other examples include:

- In 2014, the UK National Crime Agency reported that 650 people were arrested for accessing child abuse images online. Many of these people were from highly respected professions, including teachers, medical staff, former police officers, a social services worker and a scout leader.
- Professional gaming is highly popular in South Korea, where the best can earn ‘hundreds of thousands of pounds every year’. A South Korean man addicted to online gaming suffered repetitive strain and injured his muscles as a result, deforming them and making surgery the only option to save his illustrious career as ‘the best player in StarCraft’.
- Ellen Pao, described as one of Silicon Valley’s most prominent women, resigned as interim CEO of Reddit, the entertainment, social networking, and news website. She was targeted for months with racist and sexist threats and commentary, mainly generated by online users on a website which promoted free expression at any cost.

Why would employees, or customers, or individuals behave online like this yet act benevolently offline? Dr Zimbardo, a professor at Stanford University, conducted the notorious Stanford prison experiment in 1971 which examined the psychological effects of becoming a prisoner or a prison guard. The experiment stopped after just six days, when participants adapted to their roles well beyond Zimbardo’s expectations; the guards became highly authoritarian and subjected some prisoners to psychological torture.

Shocked by this transformation, and by similar behaviours at the Abu Ghraib prison in Iraq in 2004,
Zimbardo questioned why seemingly good people turned to evil behaviours in his book *The Lucifer Effect*. In this book, Dr. Zimbardo defines evil as ‘intentionally behaving in ways that harm, abuse, demean, dehumanize or destroy innocent others – or using one’s authority and systemic power to encourage or permit others to do so on your behalf’. Dr. Zimbardo defines two types of evil: essentialised and incrementalist (see Table 1 on the next page):

The traditional focus for adverse online ‘human’ activities in corporate cyber security has been on ‘insider threats’, defined as ‘a person who exploits, or has the intention to exploit, their legitimate access to an organisation’s assets for unauthorised purposes.’ Examples of this can include dishonest employees stealing money or sensitive information within their organisation’s IT systems for personal gain or revenge. In most cases, the motivation has been solely to identify and remove the insider threats as quickly as possible whilst causing minimal damage to the organisation’s assets and reputation.

It may be much harder for both organisations and individuals to accept an alternative ‘incrementalist evil’ perspective, which upholds a view that we are all capable of adverse online activities, depending on our changing circumstances and perspectives (‘we all could become those bad apples depending on where we sit in the barrel’).

It may be tempting at this point to claim that online incrementalist evil is nearly impossible to mitigate, let alone through cyber risk management. I would however suggest that it can play a part by helping to identify and manage any inconsistencies between how management, employees and individuals behave online as well as offline.

Beyond just identification, management, employees and individuals need to own and be accountable for these types of risks both at an individual and systemic level. Cyber risk management needs to recognise that the online workspace blurs professional online activities with personal ones and that cultural factors, not just IT factors, play a critical role in managing cyber risks.

There are significant opportunities that can be identified by businesses, organisations and individuals in response to online incrementalist evil. Senior management within businesses and not for profit organisations can set the tone online and positively impact on how other employees communicate. Clearer policies and governance around online behaviour can provide reassurance and improved morale for staff. Combined with this, cyber opportunity management can work with businesses and individuals to identify and exploit positive social initiatives online to help both the victims in the workplace (e.g. the Cybersmile Foundation www.cybersmile.org) and employees with internet addictions or adverse online behaviours.

Whilst cyber risk management can identify risks about the darker side of human nature in online activities in the workplace, it can also highlight the opportunities of positive online behaviour at the same time and therefore help employees enjoy the online world at work safely, more fully and more effectively.

**Table 1: Essentialised and Incrementalist Evil**

<table>
<thead>
<tr>
<th>Type of Evil</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Essentialised</td>
<td>• Deflects responsibility away from other individuals in the organisation</td>
</tr>
<tr>
<td></td>
<td>• ‘There will always be a few bad apples in the barrel’</td>
</tr>
<tr>
<td></td>
<td>• ‘It’s the way of the world – we can’t change it’</td>
</tr>
<tr>
<td>Incrementalist</td>
<td>• Recognises that responsibility may be present in every individual</td>
</tr>
<tr>
<td></td>
<td>• It may even have systemic causes with senior management setting the wrong</td>
</tr>
<tr>
<td></td>
<td>tone or turning a blind eye to adverse online activities (looking beyond the</td>
</tr>
<tr>
<td></td>
<td>‘bad apples’ to the designer of the apple barrel).</td>
</tr>
</tbody>
</table>

References

2. See UK London Evening Standard, Tuesday 21st July p.15
4. See http://www.bbc.co.uk/news/uk-28326128
5. See http://www.bbc.co.uk/news/technology-32996009
9. See http://news.bbc.co.uk/1/hi/8493149.stm
Rethinking reputational risk

ANTHONY FITZSIMMONS

Reputations are universally seen as important and valuable, but reputational risk is poorly understood. As a result, reputations are left unnecessarily at risk.

Historically, risk managers and internal auditors struggled to define reputational risk. Some saw it as the ultimate result of the failure of the organisation to manage other risks properly. Others saw reputational risk as a separate category of risk in its own right. What united both groups, and business leaders, was the view that reputational risk was the most serious risk facing their organisation; and that they had to avoid the kinds of outcomes that had regularly plagued and destroyed reputations in the past.

If a fashion retailer sources stock from a manufacturer that uses child labour, pays its what consumers see as exploitative rates of pay or provides dangerous working conditions, the retailer’s reputation is at risk and likely to be damaged when consumers and their proxies the media find out. Companies that might face this or other problems that have already happened regularly recognise related areas of reputational risk.

This backward-looking approach is fundamentally inadequate. Reputational damage does indeed happen when an organisation fails to manage other risks properly. But when root causes are considered, the deeper insight is that reputations are usually lost when stakeholders come to believe that the organisation is not as ‘good’ as they previously thought.

So what is reputational risk? To arrive at a sound answer, we need first to ask what reputation is. A useful working definition is:

‘Your reputation is the sum total of how your stakeholders perceive you’

This deceptively simple statement implies six important observations:

• Your reputation is not about how you perceive yourself; it is about how your stakeholders perceive you
• Your reputation is about how others perceive you to be, not the reality of your true nature
• Since your stakeholders hold that critical perception, if your stakeholders come, rightly or wrongly, to perceive you in a different way, your reputation changes
• That ‘sum total’ can vary depending on which stakeholders are most relevant or influential at any particular time
• It is therefore important to understand all your stakeholders including when their perceptions may become more or less relevant, influential or vocal
• You lose your reputation when stakeholders come to believe, rightly or wrongly, that you are not as good as, or worse than, they previously believed you were

The definition does not help as to what perceptions matter; but the research vividly illustrates how reputations are lost when stakeholders come to think that an organisation does not meet their expectations. When it comes to organisations and their leaders, performance of core activities matters. But so too does revealed characteristics such as ethos, culture, trustworthiness, honesty, humanity, competence, the operation of incentives and the ability to learn as well as whether the organisation itself is coherent or dysfunctional.

Our research suggests that a succinct working definition of reputational risk is therefore:

‘Reputational risk is the risk of failure to fulfil the expectations of all of your stakeholders in terms of performance and behaviour’

This definition emphasises the root causes of reputational damage, which are all to do with behaviour as well as performance.
Thus revisiting the clothing retailer example, superficially the reputational damage may be due to the use of child labour, exploitative rates of pay or dangerous working conditions. But looking deeper to root causes, these causes may be the result of risks from:

• The strategy of the company (e.g. buy as cheaply as we can)
• The ethos of the company (e.g. source cheaply – I won’t ask questions about/don’t want to know how you achieved it),
• Internal incentives (prioritising cost saving above ethicality),
• Leadership which doesn’t think about ethicality at all
• Other individual or collective behaviours or features of the way the organisation is put together.

Understanding these root causes, and dealing with them, will not just prevent a recurrence of the same problem. It will prevent new problems with similar root causes you may never have thought of until they hit you. Understanding them also provides forward-looking risk insights. That is how aviators have made commercial aviation so safe, that the most dangerous leg of a long overseas trip is usually the journey to the airport. Unfortunately these risks are difficult to find and regularly lie unrecognised for years before giving the board an unpleasant surprise.

This insight is now increasingly recognised. It lies at the root of the latest Financial Reporting Council Guidance on Risk; and at the root of the growing emphasis by financial regulators on human behaviour as the origin of all financial failures.

Rethinking reputational risk, and particularly the behavioural and organisational risks that are its deeper drivers, gives organisations a valuable opportunity. Used well it provides a future-facing radar. This makes it possible for leaders and their risk professionals to find and tackle deep-rooted, well-hidden root-cause risks before they cause damaging outcomes that a conventional take on history cannot predict.

Our experience is that most business leaders have a narrow view of reputational risk; and they are unaware of behavioural and organisational risk and their implications. So are many in risk teams. This is in part because behavioural and organisational risks are recent additions to the risk lexicon and not all risk professionals yet understand them.

That is why the UK Financial Reporting Council guidance on risk explicitly sets out to encourage boards and risk teams to learn about these risks as a prelude to finding and dealing with them. With sound education and training in the field, these lethal but under-recognised vulnerabilities can be understood, found and fixed: before they cause harm.

HOW TO DESIGN YOUR OWN RISK MATURITY MODEL

DOMENIC ANTONUCCI

My new book Risk Maturity Models: How to assess risk management effectiveness opens the opportunity for any size organization to design and build their own tailored Enterprise Risk Management (ERM) maturity model - at low cost and effort and with a host of accessible resources. A powerful tool for any organization.

An organization’s size, resources or budget should not stop it from tailor-designing its own risk maturity model. The highest purpose is to gap-assess risk management system effectiveness to your unique organization. It does not mean you have to create something absolutely new, perfect or become a creative genius. It does mean understanding some basics then synthesizing what models and using the treasure trove of reference sources available to arrive at what you need to get started. Designing means a
plan to show the construction, function and workings of the risk maturity model. Tailoring means its fit-to-organization objectives, internal and external context and risk profiles.

You can start by using a simple spreadsheet matrix format to build up basic content components in three steps. We can summarize them in this sequence as: Components = Domains + Capabilities + Scales + Levels.

**DESIGN STEP 1: MATRIX YOUR PREFERRED CAPABILITIES**

Open up a new spreadsheet matrix and title it. Enter your choice of ERM capabilities on your spreadsheet as rows along the y-axis (left side). To start ‘bottom-up’, create a long list of unsorted capabilities of interest to your organization down your first column. If they lend themselves over time, sort them into a sequence if one follows another by their nature and/or sort into groups by any shared themes (such as People, Technology and Process).

Alternatively, you may start ‘top-down’ with themed capability modules then break these down into underlying capabilities and add more over time. For example, the ISO 31000:2009 standard has a core process called Risk Assessment. This can be broken down into three sub-processes of Risk Identification, Risk Analysis and Risk Evaluation.

An easy alternative is to adapt an existing spreadsheet model that is already built, web-accessible and easily tailored to your own organization. For example, you can download a Supply Chain Risk Maturity Model in soft spreadsheet format for free (with the kind permission of The Supply Chain Risk Leadership Council (SCRLC) website at http://www.scrlc.com/) and adapt its content.

**DESIGN STEP 2: RATING USING RATING SCALES**

Here is one simple rating approach. Enter a date for the latest rating. Rate each capability with a current score between 0 and 4. The numbers represent five-point scales which are typical in the market (also called Likert Scales). These can be sub-totaled (sub-index) and given a percentage completion score for each module, then an overall maturity score (total index).

The trick here is to ensure that the five-point scales are given clear text descriptions so that assessors can stay true to a common scoring system.

One readily available guidance for the five-scale rating is the HB158:2010 recommended scales. In summary, they are:

- **None = score 0** – Very little or no compliance with the capability requirements in any way
- **Very Little = 1** – Only limited compliance with the requirement. Management supports the intent, but compliance in practice is poor
- **Some = 2** – Limited compliance with element statement. Certainly agree with the intent, but limited compliance in practice
- **Good = 3** – Management completely subscribes to the intent, but there is partially complete compliance in practice
- **Complete = 4** – Absolute compliance with the element statement – in intent and in practice – at all times and in all places

**DESIGN STEP 3: RATING YOUR MATURITY LEVELS**

Now denote your aspirational or target risk maturity levels. Total up your ratings of 0-4 to a ‘Total Assessed / Total Potential Assessed = % Index score’. Divide the 100% overall potential score into five blocks of percentiles (called quintiles) and assign an ascending maturity level title with its criteria to each block.

Define your own set of tailored maturity levels. There are a host of these accessible by Google search. Now, where does your actual rating place your organization by maturity level? A simple example is below:

1. 80-100% RiskSmart: Embedded practice consistent with recommended practice. Continuous improvement.
3. 40-59% Maturing: Some ability to demonstrate recommended practice. Some opportunity for improvement.
5. Under 20% Ad hoc: Inability to demonstrate adherence to recommended practice. Fundamental need to address.
Best practice is increasing the focus on resilience against severe events, interconnected risk events, and ‘a very bad quarter’, adding to the traditional ground of limiting the occurrence and damage of risks events. Applicable in all organisations, the distinctive feature of Operational Risk Management is to:

- Extend systematic risk management
- Integrate risk evaluations
- Assess the aggregated risk exposure of the organisation

These estimations are not only in relation to single occurrences but importantly to losses in a period of time (typically a year) and, in order to know the potential for severe and extreme events, one in twenty- or fifty-year outcomes for losses. (Banking and Insurance regulators require such exposure assessments of individual or aggregate losses at very much less probable levels but very much more damaging.)

These developments have led to significant advances in quantitative techniques, especially for:

- Addressing the potential for extreme losses
- Assessing interconnected risks
- Aggregating exposures.

This is bringing information and advice to boards and directors about issues of corporate concern for their decision. This is in addition to the usual information about balancing the expenditure on controls with the potential losses, and optimising between the various risks.

Importantly, focus on the potential for major losses is a tool in anticipating important emerging risks. For example cyber-attacks are now at a much higher level of aggression, and systematic assessment of potential attacks improves the preparedness, responses and resilience of corporate and business units. It ensures the resources to limit the exposures are adequate and used to greatest long-standing effect.

As illustrated above, integration and aggregation gives new impetus to risk strategy and appetite (tolerance, as some prefer). The ability of the board to define limits to exposures for different types of risk is greatly enhanced by the better understanding of the total risk portfolio and potential for some risks to create major losses. In turn, the enhanced statement of risk strategy and appetite provides the means to re-optimise controls, whilst the standards against which to monitor changing exposures of important risks influences the review of corporate aims.

Many disciplines say their activity needs to be controlled by the CEO. Risk is developing as a discipline that demonstrates direct worth to the directors at all times. Through the important messages it can now deliver, it is becoming required information by CEOs and directors.
Defining Risk Appetite and Attitude

Risk appetite is a vitally important concept in the practice of risk management. However, it is a very difficult concept to precisely define and apply in practice. Risk appetite is sometimes considered to be defined by the risk criteria established by the organization. This is the next phase of the risk management process after the risks have been rated in terms of likelihood and impact.

Risk appetite is the immediate or short-term willingness of an organization to undertake an activity that involves risk.

Risk attitude and the risk criteria represent a longer-term view of risk.

This is much the same as the way in which a person will have an immediate appetite for food and a longer-term attitude towards food.

One of the fundamental difficulties with the concept of risk appetite is that, generally speaking, organizations will have an appetite to continue a particular operation, embark on a project or embrace a strategy, rather than a direct appetite for the risk itself.

In other words, risk appetite and risk exposure should be considered as a consequence of business decisions rather than a driver of those decisions. The decision on risk appetite is normally taken within the context of other business decisions, rather than as a stand-alone decision.

Taking Managed Risks

The typical advice in most risk management standards is that risk should not be managed out of context, so questions about the risk appetite can only be answered within the context of the strategy, tactics, operations and compliance activities being considered.

Many commercial organizations make adequate profits but take too much risk or make inappropriate use of the risk capacity of the organization. Risk capacity, or the capability of the organization to take risk, is not the same as the cumulative total of all of the individual values at risk associated with the risks facing the organization.

By contrast, risk appetite is the total value of the corporate resources that the board of the organization is willing to put at risk. Most organizations have not determined the value they should risk (risk appetite), nor calculated how much value is actually at risk (risk exposure), nor the capacity of the organization to take risk (risk capacity).

Optimal Risk-Taking

An organization should be able to decide how much it wishes to put at risk, based on the organization’s attitude to risk. Agreeing the risk appetite will ensure that the organization does not put too much (or too little) value at risk. Risk taking needs to be at the optimal level and deliver maximum benefit. Similarly, the organization should not put more value at risk than is appropriate, given the sector in which it operates and prevailing market conditions.
The portion of risk appetite that is associated with opportunities can be considered as the opportunity investment that the organization is willing to embrace. They will be willing to invest resources in opportunities that potentially lead to positive gain. However, the organization should recognize that more value can be destroyed by incorrect strategic decisions than by hazard, control or even compliance risks. Careful identification of the nature of the risks and calculation of the actual risk exposure associated with the opportunity should be undertaken.

A CASE OF TWO MANAGERS: DIFFERENT APPROACHES TO MANAGING PEOPLE RISK

KEITH BLACKER

Imagine you are the CEO of a large multinational company and it is appraisal time. It’s been a busy year and the business has had to cope with a large number of projects which have been necessary to help secure the future development plans of the organization. Amongst these are a number of e-commerce projects. You decide to review a couple of the appraisals for two of the project managers, one who whom had implemented the system on time, while the other hadn’t. Here’s how they sum up their performance:

THE RISK TAKER:

‘Well, I know that we had to cut a few corners on the way to making this project a great success but if you were in my shoes you would have done exactly the same. Let’s not forget, we managed to implement the new e-commerce system in just twelve months with staff working around the clock, and nobody believed we could do it. A few customers may not return as we continue to iron out the remaining bugs, the paperwork is behind and the press picked up on the teething problems we originally had, but despite the problems, I know the company will be pleased with the admittedly lower than expected profit we’re now generating and I’m looking forward to a significant bonus.’

So, what would drive the two project managers to display completely different behaviours in the same organization? And who do you think deserves a bonus?

THE RISK MANAGER:

‘Whilst I appreciate that we are six months behind schedule with our implementation of the e-commerce system, we need to look at the bigger picture. The most recent survey of the project team illustrated how highly motivated the staff are, with all of the training schedules fully met and the project documentation being marked as excellent by the quality assurance team. Most importantly, we are fully compliant with the recently introduced corporate guidelines on work-life balance; the first team to do this. Despite being behind schedule, I know the company will be pleased with all the hard work we have put in and I’m looking forward to a significant bonus.’
message for frontline managers to understand. It matters because if culture is not actively managed, it can create a climate in which risks, and people risks in particular, can emerge and grow. There are numerous examples of where the word ‘culture’ has been used as a reason why a major disaster has happened; for example, the Columbia Space Shuttle disaster and BAE Systems.

A GOOD RISK CULTURE

What are the things that make a good risk culture, i.e. a culture that helps all staff to understand the importance of risk within the organization? In short, many things, some of which are illustrated in this article from the same authors: ‘What Makes a Good Risk Culture’?

Having a good risk culture will not prevent people risk events from happening – all it can do is hope to reduce their likelihood (to as close to zero as possible). This raises the question as to what is going to cause an event to take place and is there anything that can be done to prevent it? We are, of course, discussing people, their fallibilities, their foibles and those ‘hard to control things’ that influence the way they behave at certain times. We all have bad days, we all miss things, we all avoid things, we all fear things; we are after all human. The best we can hope to do is recognize that mistakes are more likely to be made when individuals:

- are overworked or underworked;
- are tired;
- are stressed;
- are overconfident or underconfident;
- are forgetful;
- are complacent;
- are in the wrong job;
- have been promoted above their level of competence;
- have problems at home;
- have different priorities (to doing their work)

Returning to our two managers, every organization is likely to benefit from having individuals who lean towards being Risk Takers/Risk Managers when it comes to risk management. Why both? Imagine the organization as a car and the accelerator pedal represents the business moving forward and taking risks, whilst the brake pedal represents the business holding back and managing risks. If you are going to drive the car well, you need both pedals to work and people to operate them.

WHAT IS RISK CULTURE AND WHY SHOULD WE CARE ABOUT IT?

ALEX HINDSON

Enterprise Risk Management (ERM) has been under the spotlight since the 2008 financial crisis, particularly in the financial services sector. The question is often asked, ‘where was ERM?’ Too much focus on process and regulatory compliance has seen ERM devalued.

Risk culture can be seen as part of the answer. Culture in many ways is ‘what staff in your organisation do when you are not watching them’. Risk culture, is therefore values-based and ethically driven rather than based on processes or formal governance. When the chips are down, experience has suggested that culture trumps process every time when it comes to determining whether risk management is successful.

Why does this matter? All organisations have external stakeholders who have considerable influence over how it perceived and its future prospects for success. Since the financial crisis in 2008 public trust in companies has dropped. Regulators have reacted by increasing their scrutiny. Recent examples include the Financial Reporting Council guidance on risk management highlighting the board’s responsibility for defining the ‘culture it wishes to embed in the company, and whether this has been achieved’. The Financial Stability Board has also issued guidance on how to approach the analysis of risk culture of
financial services organisations.

What does this mean in practice for risk functions? It means a need to take a more holistic view of implementing risk management in their organisation. Creating or shaping a more risk-aware culture is, however, potentially the greatest value a risk function can bring to the table in terms of preparing their organisation for the challenges of uncertain and fast-changing environments.

A practical case study outlines how this was applied in practice to a financial services institution to demonstrate the importance of establishing a change management plan for risk culture. The Institute of Risk Management (IRM) has developed a toolkit for diagnosing an organisation’s current risk culture, completing a gap analysis and implementing a structured improvement plan. The case study demonstrates the importance of gaining board sponsorship for any such programme and ensuring management buy-in to the objectives. This organisation adopted three different tools advocated by the IRM to investigate and drill-down the root causes of the current risk culture. High-level desk-based analysis was supplemented by an employee online survey and a small number of structured targeted interviews.

The overall outcome of the project was a report, presented to senior management and the Board outlining areas of strength and weakness in terms of the alignment of culture with corporate values, and a number of practical improvement actions, that could be sponsored by the Committee.

This then enabled a cross-functional team involving Risk Management, Communications, Human Resources to put together a structured change management plan to guide the organisation towards its new culture goals.

An organisation with a risk-aware culture is one that is more resilient to external influences and better able to adapt. The benefit of a strong risk culture derives from agile decision-making in terms of the risk and reward of different opportunities. Less unenforced errors arise from a risk-aware organisation able to learn from previous events and mistakes and improve its processes in a timely manner.