www.campbelltickell.com Campbell Tickell @campbelltickell1

ctBRIEF Risk & assurance

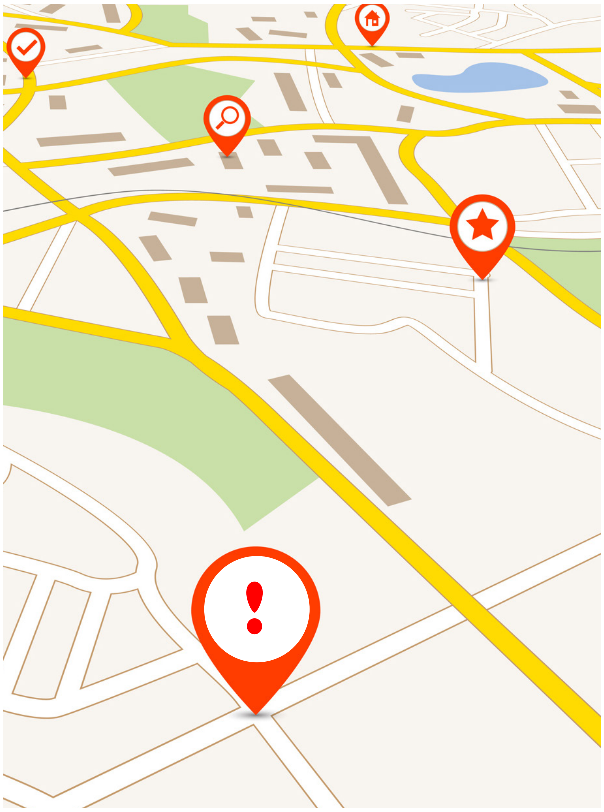
November 2017
No. 31

Sue Harvey director, Campbell Tickell

Learning to love the corporate risk map

THIS ISSUE

To discuss how Campbell Tickell can help with the issues raised in this edition, please email sue.harvey@campbelltickell.com



Shutterstock

"At Campbell Tickell we have reviewed a huge number of corporate risk maps. We've seen some excellent examples and many poor ones. Here are our six tips for getting it right.

1. Keep the map presented to your board short. Faced with a longlist in a tiny font most board members will barely register what it contains and stand no chance of picking out what has changed since last time. This sorry situation will be made even worse if what was designed for an A3 page is presented on the screen of a small tablet.

It follows that the trickiest bit of agreeing a risk map is walking the line between being too granular and too vague. If 'government policy' is one of your top risks, there will inevitably be many different impacts and it will be hard to shape the most appropriate mitigations. But if the definitions are too granular, the board will be back looking at a very long list. Hence you need a clear framework for delegation and escalation to give the board confidence that it can let go of risks ranked (say) 9 to 59.

2. The impact assessment should calibrate the relative scale of each risk, showing for example that the inability to raise £25 million in six months to fund growth ambitions is a far greater risk than a social enterprise subsidiary failing to match last year's operating surplus of £10,000.

Once evaluated, the risks should be ranked by the residual risk. By all means map the key risks to the strategic objectives somewhere, but that main list must show the biggest risk at the top.

"Avoid relying on 'monitoring' as a mitigation. You won't mitigate a car crash by observing closely as it happens."

3. Accountability. Clearly identify who is accountable to the board for the management of each risk. That responsibility should lie with a single role, not with a group of people. If nobody or everybody is accountable, then that risk will not be effectively managed.

4. Use the risk map to drive a conversation between the board and the audit committee. Boards: ask your audit committee for assurance that the key risks are being effectively managed in line with your risk appetite.

Audit committees: use internal audit, specialist advice and regular deep-dives to provide that assurance. And prioritise poking a stick at those controls which are doing more of the heavy lifting, as indicated by the gap between the inherent (gross) and residual (net) risk.

5. A personal bugbear, please avoid relying on 'monitoring' as a mitigation. You won't mitigate a car crash by observing closely as it happens. An action is required to reduce either the likelihood or the impact or both. A control that reduces neither the likelihood nor the impact is not an effective control. In a similar vein, a control that is not yet in place cannot impact on the residual

Continued on page 2

Edited by Stuart Macdonald and Zina Smith

Elizabeth Sandwith chief professional practice adviser, Chartered Institute of Internal Auditors; chair of Audit & Risk committee, Leeds and Yorkshire Housing Association

Internal audit at the heart of top organisations

Chartered Institute of Internal Auditors

"Trust in business is at an all-time low. There has been crisis after crisis. The now famous WorldCom and Enron scandals occurred almost 20 years ago, yet this wasn't the end of corporate failures. Just last year BHS and Sports Direct came under scrutiny in the UK, and Wells Fargo in the US.

The UK general election in May saw the three major political parties pledge to reform corporate governance. In addition, earlier this year the FRC (Financial Reporting Council) announced a review of the Corporate Governance Code.

The challenges and risks facing businesses are not only external. Whether it's the fluctuation of Sterling, extreme weather conditions or the uncertainties surrounding Brexit, businesses face a whole catalogue of risks.

So, in this ever-changing environment, how does internal audit contribute to improving the trust customers and staff have in the organisations they deal with?

Business today is characterised by change, complexity and crisis. This provides both challenges and opportunities for organisations and, while being ready to respond is essential, it's not easy. Internal audit has emerged as an important means of giving boards and other key stakeholders the confidence to deal with the demands of a dynamic marketplace.

Internal audit can be best described as an independent evaluation as to whether an organisation's risk management, governance and internal control processes are operating effectively. With more and more organisations, and CEOs, relying on internal audit to enhance and protect organisational value by providing risk-based and objective assurance, advice and insight, what impact does this have on the way internal auditors conduct their work?

It often means that the head of internal audit (HIA) sits at the top table i.e. the board. This allows the HIA to build their knowledge of the business and help provide assurance in relation to the strategic risks facing the business. The days of internal audit focusing on petty cash are long gone!

Another result is that the relationship between internal audit and the risk function is stronger than ever. Together, these functions are able to assess the risks facing an organisation to help achieve its strategic goals and objectives. In addition, they are able to assess whether the risks are appropriately mitigated but also ensure that opportunities are not overlooked.

"Together, the internal audit and risk functions can assess the risks facing an organisation to help achieve its strategic goals."

As expectations rise, internal audit is responding by increasing the value it delivers. The highest performing internal auditors – those adding the greatest value to their organisation – not only deliver on their core mandate of providing assurance, but also aspire to deliver value as a trusted advisor, or act as a critical best friend.

Internal auditors contribute to ensuring that organisations comply with the rapidly changing regulatory landscape and seek to keep itself and all of its employees at the top of their game. Ultimately, internal audit is at the heart of an organisation, ensuring it has the ability to survive in a competitive business environment, and continue to prosper. It is as simple as that.

Shutterstock

Sue Harvey

Learning to love the corporate risk map

Continued from page 1

risk. You haven't reduced the risk of a car crash today by booking in an MOT for tomorrow.

6. Triangulation. Are there clear links between your strategic risk map, your stress testing and the contingent liabilities that appear in your asset and liability register? Have you stress-tested the relevant swap rate falling to zero, the housing market shutting down, the DevCo getting into a pickle or the failure of a significant contractor?

Today anybody that wants to build more homes must manage increased risk, and the board's risk competency is a critical influence on those objectives. Short, precise, prioritised risk maps enable a board to relate key decisions and strategies to their risk appetite. The resulting high-quality debate will enable the confident delivery of those ambitions.

Sue Harvey chairs the Audit and Risk Committee of the Housing Ombudsman and co-chairs HouseMark's Business Assurance Club.

Kelsey Walker assistant director regulatory operations, Homes and Communities Agency

Is your board an intelligent client?

Homes & Communities Agency

"Is it ever a good enough defence for a board to say simply: "We took advice"? To my mind, the short answer is: "No". It is great when a board is self-aware enough to realise it needs help. However, there is little to be gained from a board asking for advice if it doesn't ask for the right advice, or if it doesn't understand the implications of that advice.

The key point here is that board members must understand the difference between advice and assurance. The former relates to options and recommendations, while the latter concerns the effectiveness of policies, procedures and controls.

A board cannot divest itself of its responsibility to manage its key risks. It cannot hide behind third-party advice or transfer its responsibilities for assurance. It needs to have enough knowledge to take and act on appropriate advice, be clear on the assurance it is looking for, and be prepared to take decisions based on that assurance – an informed, iterative process. In short, it needs to be an "intelligent client".

How is a board to know when it is falling short in this duty? This is best illustrated by some examples from my regulatory experience.

One board didn't have treasury skills, so it bought in advice. But it didn't know what to do with that advice, which usually consisted of a range of options. It simply did not have skills to act appropriately. It wasn't able to demonstrate it was in the right place for an upgrade from G2.

Another board accepted an audit scope on gas servicing which didn't include how gas appliances were identified and added to the database. It consequently received regular assurance that gas checks were carried out on known appliances, but had missed a whole load that hadn't been identified. The problem here was that the board, through its audit committee, didn't understand the risk fully. It ended up with a serious detriment notice.

On the other hand, I recall a board commissioning a governance review (with input from the regulator), specifically to focus on financial oversight. The review was delivered within a tight timescale. It was clear upon reading the assurance report that the key questions hadn't been answered. The chair and chief executive immediately told me that they hadn't gained the assurance they wanted from the review – and I knew then that they were operating as an "intelligent client", clear about what they wanted and able to question when they hadn't got it. They were on the path to a G1.

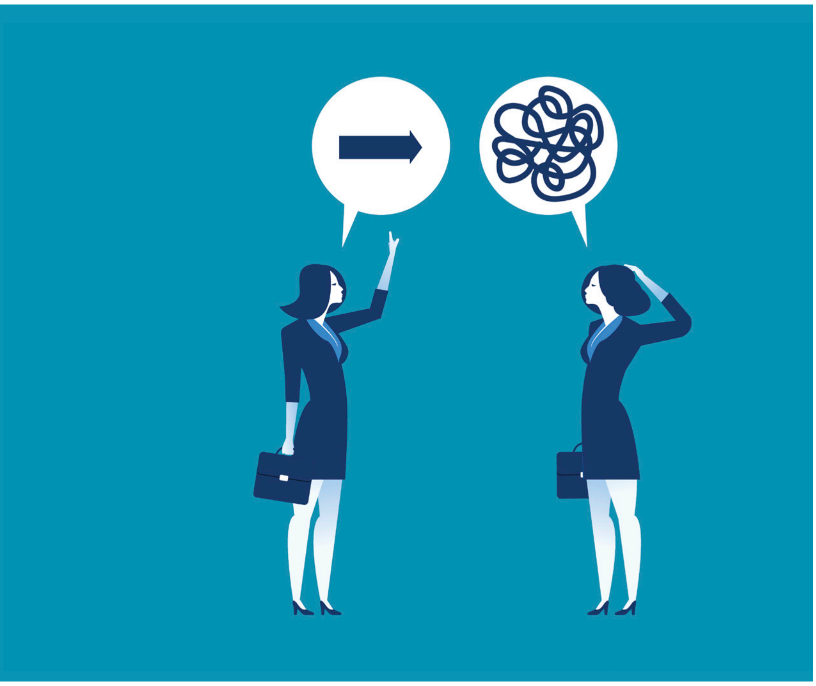
Contractual failure has crossed my desk on more than one occasion. One board's initial response was that: "We acted on advice. It was the contractor's fault." However, as I have identified, accountability remains with the board to ensure key risks are managed, core services delivered and wholesale failure avoided.

In hindsight it is easy to question how the board fulfilled its fiduciary duty to maintain systems of control if there were no poor performance clauses in the contract. Risk had not been properly identified and managed, resulting in a number of adverse consequences.

So a board's duty is to manage risks, taking and acting on appropriate advice if necessary and satisfying itself that it has appropriate assurance that controls are in place. Being an "intelligent client" is fundamental to this.

Sometimes things go wrong. We of course accept that. Leadership teams, boards and the regulator need to understand whether the failure was due to a lack of control / insufficient assurance over a higher-risk area; or non-compliance with established controls, picked up by management oversight. The answers to those questions – and the materiality of the failure – can be the difference between a G1, G2 or G3.

"There is little to be gained from a board asking for advice if it doesn't ask for the right advice, or if it doesn't understand the implications of that advice."



iStockphoto

Kathy James senior associate, Campbell Tickell

Risk culture – playing your cards right

CAMPBELL TICKELL

"As councils, housing associations and charities take on more commercial risk, how can we encourage innovation and entrepreneurship without unwittingly building a casino on a stack of poker cards?

Within organisations we tend to be good at setting up processes and systems that manage risk, but are often less good at considering the softer, cultural side of risk, those all-important behaviours and attitudes. While risk culture is generally recognised as important, it is often relegated to the "too difficult" pile. So what is risk culture and why does it matter?

Risk culture is a term describing the "values, beliefs, knowledge, attitudes and understanding about risk shared by a group of people with a common purpose". This varies between individuals, departments and organisations.

Many corporate meltdowns have demonstrated that without a positive and embedded risk culture organisations can be rocked by scandals and ultimately failure. Think of the banking crisis, LIBOR fixing and The News of the World to name but a few. This is also true in the non-profit sectors, where the lack of effective challenge on boards and a culture that did not support speaking out has often led to entirely avoidable results.

"A poor risk culture is not always one which encourages taking too much risk. Sometimes it can be a culture that prevents opportunities from being seized"

Housing professionals tend to be "data rational", focusing on what can be quantified and managed. However, it is often the intangible risks relating to reputation, people and change that can significantly impact an organisation, positively or negatively. There is therefore a business imperative that this aspect should be considered.

Public and voluntary sector professionals need to take risks to achieve their objectives. Yet risk culture significantly affects the capability to take strategic risk decisions, respond to arising issues proportionately, and deliver on performance promises.

A poor risk culture is not always one which encourages taking too much risk. Sometimes it can be a culture that prevents opportunities from being seized and stifles innovation with too many controls and systems. A healthy risk culture will lead to the right behaviours and ethics, which in turn will encourage people to do the right thing in the right way.

What does a good risk culture look like? The Institute of Risk Management suggests that "an effective risk culture is one that enables and rewards individuals and groups for taking the right risks in an informed manner".

Eight key components of a good risk culture include:

1. Leadership
This should include a positive tone from top. Leaders should be engaged and the culture clearly communicated. A positive risk culture should work within the context of the strategic objectives, and motivate people to do the right things for the business rather than themselves.

2. Tick the box – miss the point!
A key question for any organisation is ' is the risk culture delivering the behaviour we want?' We would suggest that risk management is not just about compliance and meeting regulations. It should be aimed at proactively managing risk, with conscious risk-taking encouraged, outcomes monitored and timely remedial action taken when and if required.

3. Effective challenge
An effective risk culture will facilitate constructive challenges in respect of activities and control functions. A key question is whether the organisation enables concerns to be voiced and whether the culture supports concerns to be voiced and constructive dissent.

4. Achieving balance
The IRM suggests that the tangible difference to the success or failure of organisations is understanding how to balance risk and reward successfully. A positive risk culture should motivate, reward and incentivise staff. Inevitably things will go wrong, but to do nothing and be risk adverse can be damaging too. Staff should not be scared to take calculated risks.

5. Openness and learning
Knowledge is power: Ensuring transparency and the timely flow of risk information up and down the organisation, with bad news rapidly communicated without fear of blame, is key to managing risk. Encouragement of risk event reporting and whistle-blowing, as well as actively seeking to learn from mistakes and near misses is also important.

How an organisation deals with bad news is also key. Ignoring, denial, distraction and defensive behaviour is rarely helpful in the long term. The earlier you know the sooner you can do something about it, even if sometimes it turns out to be a false alarm.

Continued on page 5

Shutterstock

Kathy James
Risk culture – playing your cards right

Continued from page 4

6. Clear accountability and taking responsibility
Risk culture plays a critical role in ensuring effective risk governance. There should be a common acceptance through the organisation of the importance of the continuous management of risk, including clear accountability for, and ownership of, specific risks and key controls. It should be everyone's job, not just the risk manager's.

7. Realism – nobody's perfect!
Effective risk management relies on an adequate set of controls being in place that are fit for purpose, and an organisation that is compliant with them. Key elements of managing risk are having staff who are objective and realistic about their control environment and who also take action to rectify any issues which may fall short of the organisation's appetite for risk.

8. Embrace internal audit
Internal audit should be viewed as a positive experience, there to help and improve things. All too often audit is resisted rather than embraced, and that is a missed opportunity!

"Internal audit should be viewed as a positive experience, there to help and improve things. All too often audit is resisted rather than embraced"

Gera Patel partner, Campbell Tickell

Meet your new audit & risk committee

"It never ceases to amaze me how adverts for audit committee board and chair roles often sound depressingly dull and tedious when surely, in the current environment, these are the roles that should be at the pulsing heart of an organisation!

The vacancies are often accompanied by a long profile that goes into the minutiae of requirements, describing everything in great detail. This compounds why audit committees are sometimes seen for those that like to fuss and prevaricate, and hence dissuades many potentially excellent applicants.

However, the value of a high-quality and effective audit committee has never been more critical to organisations. Their value is often represented by having a broader mix of skills, professional backgrounds, and diversity of thought around the table.

"The Audit Committee's value is often represented by having a broader mix of skills, professional backgrounds, and diversity of thought around the table."

Over the last few years, Campbell Tickell has supported a variety of clients with recruitment to numerous audit committee, board and chair roles. Our experience and market presence has helped us to identify the subtle but critical changes over that period, for clients and candidates, when it comes to finding talent for these roles.

So what are they?

1 Financial acumen is no longer the end-point, rather it is considered a starting position. We bring forward candidates who have in-depth knowledge of a particular expertise, yet who also have a more rounded offer, encompassing exposure to different regulatory environments, with varying degrees of business volatility and complexity.

The emphasis is on a broader set of business assurance and risk management skills, recognising that this experience can have many guises. We have been able to help clients better appreciate the offers from individuals from varied backgrounds, at the same time as ensuring a strong alignment to the values of the sector.

2 We sometimes see that the professionalisation of audit committees can result in a group of individuals who have the right technical skills, but perhaps lack the disposition to operate as a team.

Our selection processes place a premium on testing behaviours and attributes. This ensures that our clients see candidates who have intellectual curiosity, are able to ask the right questions of executives, in a way that supports a culture to elicit challenging and thoughtful debate. The ultimate aim here is for consensual decision-making.

3 Linked to both the above, a firm recognition that these are roles where success is rooted in understanding and working well with people, not just numbers. This is about the quality of the relationships between committee members; between committee members and executives; and between the committee and the main board.

There is an emphasis on understanding the independence and inter-connectedness of the role in relation to others and on creating an environment at the audit committee where executives are not being caught out, but instead are encouraged to be open, forthright and accountable.

At Campbell Tickell, we think this all adds up to a different conversation on how to fill those all-important audit committee vacancies.

You may be a client looking to fill pending non-executive vacancies; or perhaps you are in the market for a board or chair role. Contact us at recruitment@campbelltickell.com and we will be happy to chat, to see if we can help.

Shutterstock

Sue Harvey director, Campbell Tickell

Assurance after Grenfell

"The tragedy at Grenfell Tower has raised many immediate and pressing questions about cladding, fire doors, tower block safety and much more. While the ongoing investigations and inquiries will highlight just where things went so catastrophically wrong on 14 June, a key area will almost certainly be the role of assurances sought and obtained.

A question I have found myself asking is whether the faith the housing sector places in external assurance as the third line of defence has been seriously undermined.

There are many business-critical areas where housing providers rely on external experts to double-check adherence to legal requirements, regulations, standards and best practice. As a sector, we depend on these external experts to be both specialist and independent: to understand the technical details of their subject area and to be confident in telling us where we are not coming up to the mark.

In fire safety, all the necessary elements are in place: legislation, regulations, standards and mandatory external assurance. And yet something still went massively wrong in west London.

In this and other areas of assurance, might the housing sector have inadvertently created a tick-box process that muddies the picture rather than giving effective warning of deficiencies? Here are some of the questions that could help boards to distinguish high-quality assurance from box-ticking in future:

- **Standards** Is there a choice of standards? Why have the ones compliance is being measured against been chosen? Who sets them? How confident is the housing provider in the independence and rigour of the standards? When were they last updated? How quickly do the standards respond to new information and learning?
- **Assessments** Are the assessors, specialists, or auditors qualified and independent? Does a profession or trade body vouch for their credibility? Do they understand the context and drivers of the review, and the reliance that the housing provider will place on their conclusions? Does our brief encourage honesty? Is it sufficiently comprehensive to obtain the assurance the housing provider really needs? Are the external experts happy to expand their usual checks to accommodate specific requirements? Is there a role for the audit committee in scoping the brief and agreeing any actions? What's a reasonable frequency of updating?
- **Gaps** Are the root causes identified, rather than the presenting symptoms? Is it clear which are the most critical? Are they graded and ranked? Are the results triangulated with complaints and whistle-blowing?
- **Actions** Are they clear, specific, prioritised and resourced? Are the accountabilities and timescales clear?
- **Monitoring** Are all gaps and recommendations tracked? Are outliers, trends and benchmarks highlighted in our reporting? When should the audit committee and board be updated on progress? When should the results be shared with wider stakeholders?

The role of assurance, both internal and external, will not diminish. But how housing providers procure external assurance and the questions asked of those appointed to provide it may well alter. Grenfell Tower has demonstrated that to deliver well-placed confidence, it is necessary to take responsibility for the quality of the assurance being provided. Executive teams and boards will want to be clear about their respective roles, methods and skill sets, as each has an important and unique role to play.

This article first appeared as a blog on the Social Housing magazine website.

Securing high-quality assurance

Standards → **Assess / Audit** → **Gaps** → **Actions** → **Monitoring**

Standards
- Clear language
- Choice: reasons for choosing those we're using
- Authors: international body, legislation, central / local govt, professional body, industry body, commercial company
- Independent
- Rigorous
- Up-to-date
- Confidence of sector/ market

Assess / Audit
- Who: company or sole trader
- Understand: drivers, reliance that will be placed
- Credibility: qualifications, professional / trade body, reputation, corporate ownership of opinion
- Independence: fees from only one party, regular rotation, providing little or no non-audit services, dependence on business from us, record of delivering difficult messages
- Learning from networks, incl. int'nl, keeping ahead of changes in standards
- Understanding the reliance we will be placing on their conclusions

Gaps
- Clear language
- Root cause identified
- Consistently graded (major / minor, RAG)
- Ranked
- Correlated
- Triangulate with complaints and whistle blowing

Actions
- Clear language
- Prioritised
- Agreed by management
- Resourced
- Clear accountability, with named roles
- Timescales

Monitoring
- Tracked
- Who: authority to agree cleared
- Delegation and escalation
- Outliers, trends and benchmarks
- Transparency as discipline
- When should udit committee and board be sighted?