MARKS SATTIN

INTERNAL AUDIT

ROUNDTABLE 2019

INTRODUCTION

Our team in Leeds held an Internal Audit Roundtable at the DoubleTree Hotel, attended by a group of senior professionals in internal audit, risk and compliance, from a wide range of organisations. The aim was to discuss topics that are currently impacting their profession, and share experiences and insights.

This whitepaper distils the key points which emerged from the discussion, specifically looking at:

- Sustainability - climate change and environmental issues – what’s the reality?
- Governance - the new Corporate Governance code, internal audit’s role in risk management and auditing culture
- Is internal audit creating the right impact? We talk about report writing and responding to new technologies
- The challenges of IT security, cyber risk and GDPR

David Clamp | Senior Manager, Yorkshire
david.clamp@markssattin.com

SUSTAINABILITY

CLIMATE CHANGE AND ENVIRONMENTAL ISSUES – WHAT'S THE REALITY?

"Are businesses really engaging with environmental and sustainability issues or are they just 'box-ticking'? Is anyone auditing in this area and if they are, how are the audits being received by the business?"

These key questions were raised in our roundtable and the answers showed that many organisations are only beginning to grapple with these topics. Most organisations are doing supplier auditing but they are relying on certifications or on third parties to check what their suppliers are doing, with supplier auditing organisations seemingly deeming themselves to be automatically compliant with regards to being environmentally conscious and sustainable. When a supplier works with other big names such as Marks and Spencer, organisations are hoping that they apply the same standards to work done for them. There is also a need, when relying solely on your supplier, to consider common risks, such as increased demand meaning the supplier has to outsource.

How do organisations then gain insight into the processes of that outsourced supplier and whether they are compliant? A press article was brought to light to explore these questions further. The article was about a charity that had reported several UK companies to the Financial Reporting Council for failing to include climate change and environmental risks in their annual reports, all of which were audited by Big Four firms. This article was well known around the room. One of our participants explained how this exact article had been used as an indicator of importance when approaching the audit committee to include climate change as a principal risk for their organisation.

In recent years, there has been a lot more legislation around environmental protection and sustainability and there promises to be a great deal more in the future. When looking at larger organisations it's worth noting that they are governed by environmental reporting obligations under CRC (Carbon Reduction Commitment) legislation.

> Organisations need to educate themselves and their employees on positive behaviours and prioritise environmentalism appropriately to set them up for the future.

This, coupled with other legislation, makes it a priority for organisations to include data on energy and environmental impacts in their annual reports. It was agreed that in order for the board to be comfortable with the statistics and to satisfy an ever-growing expanse of legislation, there will need to be an audit. It was agreed that this new legislation is going to require a lot more effort.

One organisation sadly noted that: "We have to do a lot of environmental reporting but it's all about what the regulator tells us to do, rather than the company really getting on board with what more we could do, given climate change risk, and responding to that."

Another participant said that they had asked the board to produce a statement on what they wanted done in respect of the environment; did they want to be forward thinking or just to be compliant with legislation? No one had a clear response. They believed lip service was still a key component and only when there is enforcement, will organisations start thinking about it more strategically.

However, consumers are demanding change and driving environmental initiatives. We're seeing a comeback of "wonky fruit and veg" as opposed to the straight looking carrot or the perfectly round apple, and plastic bags swapped for paper due to popular demand. In response to these changes, participants hope to see "progressive CEOs" willing to do the right thing even where there's an impact on profit, although a level of "realism" is still needed, particularly at the value end of the market.

Organisations can run the risk of layering environmental issues so much that the product becomes more expensive and you're actually taking something away from your consumer. So, what about the emerging sustainability legislation? There are different mechanisms in place in organisations in order to stay abreast of these changes.

Examples include compliance and legal teams and prevention and compliance committees, who meet monthly to discuss legislation. Organisations need to educate themselves and their employees on positive behaviours and prioritise environmentalism appropriately to set them up for the future, as these issues become more of a priority. Soon lip service won't suffice and positive climate change behaviours and environmental activity will be necessary, especially to avoid damaging headlines.

GOVERNANCE

THE NEW CORPORATE GOVERNANCE CODE

As the centrepiece of the UK government's intent to enhance public trust in business, the biggest impact mentioned around the room when discussing the new corporate governance code was the shift away from emphasising shareholders and towards emphasising stakeholders. The word 'stakeholder' appears rarely in the 2016 corporate governance code – now it is highly visible.

This has led to organisations "doing all sorts of things with stakeholder engagement and meeting suppliers" in order to improve this relationship and comply with the code. Ultimately this is having an impact on audit plans and will be a bigger issue to wrestle with moving forward.

INTERNAL AUDIT'S ROLE IN RISK MANAGEMENT: WHERE IS THE LINE?

A popular topic of discussion is the intersection between risk and audit and to what extent internal audit should be drawn into setting the risk management framework of an organisation.

Among other titles, we find a lot of professionals are risk and internal audit managers and/or work in risk and internal audit teams.

This points to how "the three lines" are becoming blurred. From all the participants in the room, several said they were regularly asked to help develop risk management documentation. Meanwhile, others had noted they were working across the three lines for the first time and found it "really frustrating".

One of the main reasons for this could be that many organisations aren't large enough to support a dedicated risk management function. In some cases, as a work-round, people try outsourcing and co-sourcing risk management, but a risk function relies heavily on robust knowledge of the business and industry, and finding someone who fits the criteria on an outsourced basis is difficult.

Another consideration is the issue of safeguarding – auditors by the nature of the role "can't mark their own homework". However, participants talked about safeguards that can be put in place in order to not cross the line, such as not being present at the decision-making parts of meetings and having a governance structure which very clearly holds business risk owners accountable.

The important part is to know who owns the risk and who owns the controls, even if you set them out. One step in the right direction is the extension of SMCR (Senior Managers & Certification Regime). Before this extension, there wasn't necessarily a culture of real risk ownership and the SMCR is really going to strengthen accountability. Several participants commented that they welcomed this integration.

In conclusion, reconciling the conflicts between audit and risk is never easy. A recent Big Four survey reported that people are looking for auditors to be more helpful, especially when required to work across the three lines. Moving forward, audit professionals should expect and accept that the lines will be blurred and try to be practical and pragmatic.

However, it's seen as a very good thing that internal auditors are turned to and seen as trusted advisors with something valuable to contribute, when it comes to managing the risks an organisation faces.

AUDITING CULTURE

Organisational culture remains a hard concept to pin down, and in order to get to grips with the culture of your organisation, it's essential to conduct an audit.

Auditing culture doesn't have one fixed approach; our participants mentioned a variety of ways to get to grips with the culture of an organisation. It can be done through a dedicated culture audit, which may involve a lot of questions and a lot of management time, for a not very clear reward. On a smaller scale, audit teams can incorporate key culture questions when conducting other audits internally. Culture questions can also be asked through companywide surveys, including qualitative questions such as "Do you see yourself here in the next 12 months?" and "Are you proud to work here?" These types of questions can generate some valuable content for a culture audit.

A more subtle approach to a culture audit can be simply observing organisational culture, to pick up anything that could inhibit the changes the organisation wants to make. The participants in the room drew on difficulties arising when trying to decipher the difference between a good culture and a good line manager, and where the trouble might actually lie. This would influence where the change needs to be made.

The people in organisations can also become very sceptical of culture and of efforts to change it. Notwithstanding this, our participants felt that "tone from the top" is hugely influential in this regard.

> In order to get to grips with the culture of your organisation, it's essential to conduct an audit.

REPORT WRITING

A lot of times the work that goes into creating a report can be lost in the way it is presented. The participants commented on how they had been challenged on the way they had presented their findings to the audit committee. A question raised was whether anyone had actually asked the committee how they would like to see the information.

This sparked a discussion on some of the different ways reports can be produced, which is summarised below:

1. Software – reports are loaded onto the software which produces summary paragraphs, and these are reported to the committee. Each member has the opportunity to read a summary and, based on the contents, move directly to the specific page of interest.

2. Dashboard approach – this uses colour codes to emphasise importance, such as red for critical reports, then amber and green for less critical reports. However, this came across as a blunt tool, because each person looking at the report might have a different lens on. For example a financial report might be marked as red but be of less interest to a person who is more customer focused rather than focused on the finances.

3. Scoring approach – this is used to mark reports as either a pass or fail, based on a list of action points. Action tracking with scoring is used to look at completeness.

There are many different ways to produce audit reports. Each organisation works differently and inevitably everyone wants different things, although it would be most beneficial to ask the committee which way works best for everyone who uses the report to make business-critical decisions.

RESPONDING TO NEW TECHNOLOGIES

Harnessing digital technology is a prerequisite for optimal organisational performance. In the digital era, people's roles are inevitably changing and the head of internal audit is moving away from a purely financial and operational focus, to be more inclusive of the impact of new technology. Even in construction, site managers take deliveries on iPads, with all data being housed on a database. Either auditing needs more IT specialists or auditors in general need to acquire more IT skills to adapt to this new reality.

Organisations that are large enough now have dedicated IT auditors, separate heads of IT audit and a head of operational and financial audit, who both report into the chief internal auditor. However these larger organisations may for the moment struggle to keep a full time IT auditor busy. And even then, it was pointed out, often no single individual has all the necessary knowledge.

> “In the future, being a head of internal audit will require robust IT skills because of the growing focus on digital and the risks it holds.”

They can do generalised controls but technical specialists might still be needed for specific and advanced applications. Secondments and co-sourcing are two possible solutions, but it is difficult to find people with the right skills, secure them and meet their high salary demands. Participants did agree that the shift towards technology might not impact those working in smaller organisations, just yet.

In the future, being a head of internal audit will require robust IT skills because of the growing focus on digital and the risks it holds. At the end of the day, everything that goes on in a business, whether it's digital or not, ends up hitting financial statements, so it's still important to have people with operational and financial backgrounds, along with IT. The role of internal audit is about looking at challenges and strategic objectives, and if those are to be delivered digitally then heads of internal audit need to put their hands up or get in some help.

IT SECURITY AND GDPR

CYBER RISK

The biggest challenge with IT security is people. Having controls in place may seem an easy way to reduce risk but people can still be a weak link. By handling the introduction of people into various IT systems we can ensure, in some part, that the risk is being managed. This can come in the form of good inductions and refresher training when necessary. There are various ways to test and manage the degree of human error possible within an organisation.

One participant mentioned a phishing email test, although when implemented and flagged up in advance, 50 per cent of employees still failed. Among many other approaches, the most popular mentioned were fraud-monitoring email inboxes, where people can forward emails they're suspicious of, and switching off auto population of email addresses.

GDPR

Twelve months on and organisations are reporting that GDPR has fallen slightly off the radar for senior management. From an internal audit perspective everyone in the room agreed that although they are not necessarily being pulled into as many GDPR support issues, the risk is still there and that won't change.

Organisations need to keep up their messaging about GDPR, so employees remain aware of the issues. As one participant noted, "you can have all of the controls in place, but you have to be able to demonstrate that the person was aware of what they should do."

Complacency about GDPR would be ill-advised. Auditors still have to drive data security projects and still believe that GDPR will be a part of their annual audit planning cycle for a while longer.

It's good to remember that once legislation has been put in place and practiced, the rules will always be enforced more harshly. One participant had been told by the ICO that having had the chance to fix legacy issues and sort everything out, they will come down on breaches "like a ton of bricks".