Presentation at Audit NZ briefing 8 May 2018

Importance of Audit and Risk Committees

Good afternoon and thank you for the invitation to attend today's briefing.

I have been asked to talk about the importance of audit and risk committees to the overall effective governance of your business and valuing your audit and risk committee.

To do so I will take us on a journey as to how Audit and Risk has evolved into being a value add component of the governance model.

So to start with a confession, in my earlier career I was an internal auditor so do have quite an affection for audit and risk.

Irrespective of whether it is public or private sector, the governing body has the following functions, which are based on the IoD Four Pillars of Good Governance:

Holding Management to Account
Effective Risk Culture
Future Focus - Strategy
Effective Governance Culture

Sub committees are used as a way of keeping the wheels moving between governance meetings and providing a level of assurance to the governing body.

They do not replace or absolve governing bodies of their responsibilities. This is quite an important point to understand, the governing body is ultimately responsible for the effective governance of the business not the sub committees.

So what makes a good Audit and Risk Committee?

1. Clear Terms of Reference

What areas will the committee cover - easy to say that it is audit and risk but this needs to be clarified, e.g. where does health and safety sit?.

Rules of engagement - no decision making is the most common one
Frequency of meetings
Committee membership
Engagement with management and at what level, i.e how far down into the organisation?
Engagement with external auditors

2. Committee membership

In the context of Local Government, external or not external, independent chair or not independent chair.
Why bother with an external?
Does the external having voting rights?
Should you pay the external?

3. Frequency of meetings

When I first started work, which was a long time ago, the Audit and Risk Committee or to be fair the Audit committee would meet twice a year to review the half year and full year accounts.
As the business environment has changed and continues to change, risk has become a more prominent part of the Audit and Risk Committee.
Typically there are up to four meetings a year of the Audit and Risk committee. Clearly it is not a precise science and the meeting frequency needs to be one which is appropriate for your organisation - HOWEVER the frequency of meetings need to take account of the areas that need to be covered with sufficient time for matters to be discussed and actioned rather than some sort of factory process which does not hold management to account, does not create an effective risk or governance culture.

4. Committee workplan

Developing a workplan does help in addressing the frequency of meetings and provides clarity as to what will be covered at each meeting. The workplan helps tp drive activity rather than being passive and being in receive mode.

My preference is to have a combination of standing and meeting specific topics.

In terms of standing items, these include:

- Update on actions from internal and external audits. The emphasis in this area is update and progress. The role of the committee is to ensure that the actions are being progressed rather than simply creating an ever increasing list of actions. Whilst I may be teaching you to suck eggs, any action list should include the date when the action was first raised and a rule of thumb for me is that if the action becomes more than a year old, the question needs to be raised as to why. In some cases there is justification for an action taking longer than one year to complete. However that should be the exception rather than the rule.

- Update on the risk register

One of the roles of the committee is to provide assurance to the governing body that the risk control environment is effective.

The risk register is the foundation document for this assurance.

A couple of comments on the approach to risk management:

1. To be effective, the risk appetite must be fully understood. So basically how much risk is the governing body prepared to accept to deliver the overall goals and objectives?.

Understanding the risk appetite of the governing body is essential to ensuring that the risk environment is effective.
When developing the risk register/risk matrix it is important that the full governing body is involved, that the risks are the strategic risks, i.e. those risks which have the potential to derail the business and assess the appetite for each of those risks.
In identifying these risks, it is important to resist the urge to create a shopping list. Focus is required otherwise there is a risk that the outcome is simply a list of everything that the governing body can think about and it is then left to management and the audit and risk committee to try and make sense of this.

So to be clear the governing body has the responsibility to identify the strategic risks and agree the risk appetite for the organisation. And by the way, zero risk tolerance is not realistic. The role of the Audit and Risk committee is to monitor risk performance and the effectiveness of the mitigations.

This is a key component/role for the Audit and Risk committee - are the mitigations delivering the expected outcomes, is the risk moving in the expected direction or indeed being maintained at the agreed level. However this also needs to be realistic.

A couple of questions:

- How do you ensure that the risks are relevant/current?
- What is the process for updating/reviewing the risk register?
- How as the governing body do you stay current about emerging risks?

Example:
Show of hands. Russell McVeagh example. - what actions did the governing body take?

How do you remain current?

“When anyone asks how I can best describe my experiences of nearly 40 years at sea, I merely say uneventful. I have never been in an accident of any sort worth speaking about, I never saw a wreck and never been wrecked nor was I ever in any predicament that threatened to end in disaster of any sort”

Edward Smith - Captain Titanic

Still on the committee workplan

- Relationship with the auditors

Time alone with the auditors - is the auditor friend or foe?
“Bayonet the wounded”
Does the external auditor attend the full meeting or just for their agenda items?
Communication with the auditors - one way/two way communication, Letter of Engagement, Areas of focus.
No surprises - again move from being passive to responsive and proactive.
Role and function of internal audit.

- Interest Register

Best practice in respect of interest disclosure

The workplan should also include an annual review of performance. This is important to ensure that the committee does remain current and does continue to add value to the overall effectiveness of the organisation.
The committee should also report to the governing body once a year on the key activities and achievements during the year.

Of course it does need to be recognised that even with an effective audit and risk committee there is no guarantee that issues will not happen. So why bother?

For me the response to that is simple, having an effective framework in place will mitigate and minimise the likelihood, which in turn enables the governing body to deliver against the Four Pillars of Good Governance -
Holding Management to Account
Future focus
Effective Risk Culture
Effective Governance Culture.

Thank you.