ASSURANCE REPORTING

In this latest article in the Back to Basics series; Bev Cole will be taking us through an overview of assurance reporting. Bev is an independent consultant on Internal Audit and Risk Management and has worked in these areas within Financial Services for over 20 years.

Providing assurance is the ultimate goal of the Internal Audit department, it's why we're here. Sometimes it's easy to get caught up in all the practicalities of managing the department, of delivering the audit plan and raising issues and almost taking our prime purpose for granted. Ultimately what the Audit Committee wants from us is independent and objective assurance about how risk is being managed within the organisation.

So, starting with first principles, we must ask ourselves *what assurance is required, by whom and in what format*? For the purposes of this article, I am taking assurance to be at an overarching level rather than that provided within an individual audit report (see the Virtual Learning Centre for assignment reporting). I will focus primarily on the Audit Committee as our prime customer, but will also briefly cover other key stakeholder reporting.

1) Audit Committee

The frequency of reporting in writing to the Audit Committee will vary according to the size of your organisation and the risks it faces. For large organisations, a comprehensive annual report will be produced and almost certainly a half year report and quarterly updates as well. In addition, some departments report and track the highest materiality issues with the Audit Committee on a monthly basis. However, don't forget that assurance reporting is not comprised solely of your *written reports*; it also includes what you *report verbally* to the Audit Committee and also your conversations with the Chair of the Audit Committee.

What does the Audit Committee want to know, what are their expectations? Well this obviously varies across organisations. The first step is to *ask them*, something which surprisingly doesn't always happen! Then there is also an element of influencing them that there may be some information which is good practise within the internal audit profession which they should also receive if they've not asked for it, such as contained within the *International Standards for the Professional Practice of Internal Auditing**. And don't forget to explore what the Audit Committee is required to review within their Terms of Reference, plus the latest guidance on corporate governance. It is useful to see how your audit work may help them to achieve their wider responsibilities, either directly or indirectly.

Elements which you may wish to consider including in a written assurance report are *an executive summary*; the *assurance statements* over how effectively risk is being managed; assurance over the *clearance of audit issues* raised; information on *key issues accepted*; and assurance over the *quality and effective performance of the Internal Audit Department* itself. In my personal opinion, reports on any consultancy work undertaken by the Internal Audit Department should be provided separately to avoid any confusion.

There is also an emerging trend for integrated assurance reports, incorporating the assurance provided by other assurance providers including line management, Risk, Compliance, SOX Teams, Statutory Audit, Regulators etc. This will be covered within the section of the Virtual Learning Centre on

Working with Other Assurance Providers as it is a large subject in its own right. However, you may wish to consider highlighting and commenting on any major differences in the Internal Audit view and other assurance views provided to the Audit Committee.

a) Executive Summary

The executive summary provides you with the opportunity to highlight to the Audit Committee your overall *balanced view* of how effectively risk is being managed, plus any *specific concerns* you have which you believe are significant enough for them to be aware of and potentially take action on. Your overall view can be expressed as a *statement* or an actual *opinion*, either in words or as a 'traffic light'. My personal view is that our opinion is what ultimately we are paid for, and we shouldn't shy away from giving it. Additionally I think it is useful to state whether you think this opinion reflects an *improving or deteriorating position*.

The executive summary is also where you can *highlight trends* as well as specific concerns, for example, controls not being updated when processes change or deterioration in the level of compliance with controls. Often the executive summary is seen as a useful place to comment on issues around *governance* and *strategy* as well.

It is worth remembering that if there are material incidents that come to light in the organisation arising from control weaknesses in place at the time of your assurance report, then your executive summary could well form part of the evidence should questions be asked of Internal Audit. Knowing of control weaknesses is one thing; raising them in an audit report is another; and thinking them serious enough to highlight to the Audit Committee is yet another. It is valid for management to not only ask if Internal Audit raised any concerns, but also to ask if they shouted loud enough, to the right level of management and if they tracked the issues to ensure they were addressed.

b) Management of Risk

As part of the *International Standards for the Professional Practice of Internal Auditing*,* 'reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.'

There are a number of different *'cuts' of information* over the management of risk which can be used. These include by risk category within the organisation's risk map i.e. credit risk, IT risk etc.; by department / business area; and by process i.e. customer account servicing. You can report using the cut of information that best suits your organisation, or using more than one view. My personal preference is to report primarily by risk category as this aligns best with our remit of independent and objective assurance over the management of risk and it is also in alignment with the organisation's own reporting on risk. I would supplement this with some graphical information by department to highlight any hot spots in particular business areas.

So, what do you actually report on your chosen cut of information? I think the best way is to see this in the same way as the executive summary, but at a lower level. Therefore I would expect to see a *balanced view / opinion* on how well risk is being managed; whether this is an *improvement or a deterioration in control*; *key areas of concern*; and *emerging trends/risks*. Ideally you should provide some information on the depth of assurance work undertaken and why, although this is easier said than done, particularly as there is not always a direct correlation between the level of risk and the amount of audit work necessary to provide reasonable assurance.

Some people like to report only *statistically*, quoting numbers of reports issued, report ratings, issues raised, risks accepted etc. Others, and I would sit in this camp, prefer to interpret the results of the audit work into an overall *narrative* summary which is supplemented with statistical information.

I would like to give one word of warning about reporting statistically, and that is around the context of how you give opinions on individual audit assignments. Some organisations give an assignment opinion using *absolute* factors relating to the Group as a whole, one benefit of which is it does enable you to summarise ratings statistically (although it can underplay the seriousness of issues relating to a specific subject to local management). Other organisations give an assignment opinion *relative* to the subject being audited, which would give a misleading impression if they were statistically summarised (although it gives a better context in the assignment itself). For example, using *relative* opinions, a red rating on a low materiality subject such as Expenses may be less serious at a Group level than an amber rating on a high materiality subject such as Liquidity Management.

Within your narrative reporting, don't forget to provide *context* and to refer to factors external to the organisation, i.e. the economy and how that is impacting your risks; trends in risk incidents such as increasing cyber-attacks; and risk events hitting competitors which could also happen to you. Context also extends to factors within your organisation, such as the impact of expanding product lines; business acquisitions; organisational changes, IT developments, increasing staff turnover etc.

However you choose to cut your information and however you choose to present it, please remember that reporting to Audit Committee follows a lot of the 'rules' you use for assignment reporting. It should be *factually accurate, concise, balanced, report against the context of the organisation's risk appetite* and the *business and economic environment,* the *concerns should be clear* and it should be *supported by evidence*. Most important of all, if you have a serious concern you should say so and say why, and not hide it under the banner of being 'an opportunity for improvement' or underplay its seriousness because there are plans being drawn up to address it.

If your chosen cut of information does not include *reporting on change*, then I would suggest you consider reporting specifically on this as well as the degree of change in an organisation and how well it is managed can impact materially on the management of all other risks the organisation faces. So if change is being poorly managed, the risks which are well managed at the moment could see a deterioration going forward. The other factor to consider is reporting on the risks themselves and not just the management of them, if there is no separate risk reporting due to the small size of your organisation.

c) Clearance of Audit Issues

The Audit Committee (and your Regulator if you have one) will often ask the question '*is Internal Audit being taken seriously?'* One of the ways to assess this is to look at the clearance of issues. They will want to know *how long issues take to clear* and *whether issues are cleared within the deadline* promised by management and if not*, how often deadlines are revised*. They will also want to know that you have confirmed that the action promised has been cleared in reality and that you haven't just taken management's word for it, and that you are happy that the action has actually resolved the issue.

Reporting issue clearance is partly narrative, but is does lend itself very well to statistical / graphical reporting with one proviso. The same applies to summarising issues as summarising opinions; you cannot report them statistically if the issue classification is *relative* to the assignment and not *absolute* to the Group, unless you also include the assignment materiality as well. For example, if issue

categorisation is *relative*, then you cannot broadly report that there were, say, 100 Category 1 issues raised as it would be misleading, but you could that there were 25 Category 1 issues reported in High materiality audits, 50 in Medium and 25 in Low.

Please be careful on how you report issues with revised action delivery dates. The danger if you report against revised dates only is that the business just keeps revising the date and as far as the Audit Committee reporting is concerned they are on track. However, you can seriously annoy the business if you only report against original dates. One 'trick' is how you phrase your issues in the first place as often issues are revised following initial investigations into how long it will take, for example, to change an IT programme. In this case it is best to break the issue in two and have an action and date for the investigation and another action with To Be Advised for the changing of the software.

In your narrative reporting, don't forget to highlight any issues which are of particular concern as they are material and the action promised has slipped or is unlikely to be delivered when promised. The golden rule is *if you are unhappy with the current risk exposure and action being taken on any material issues, then highlight it*.

d) Issues / Risks Accepted

The Audit Committee (and your Regulator if you have one) will expect management to accept some issues / risks as long as they are *formally logged*, *risk accepted by an appropriate level of management* and *reviewed periodically*. They will, however, be interested in the scale of issue / risk acceptance and if you are unhappy with the issues / risks that are currently accepted. Again*, if you are unhappy with the current risk exposure on a material issue then raise it*. The *Standards* state that if you have an unresolved issue around risk acceptance, you 'must report the matter to the board for resolution.'

e) The Quality and Effective Performance of Internal Audit

In order for your Audit Committee to discharge its responsibilities effectively, it will want to know how effective Internal Audit is. So how can you demonstrate your effectiveness? Some things you may wish to consider reporting on are *delivery of the audit plan; achievement of key performance targets*; the *results of quality assessments and feedback*; *issue clearance and issue acceptance* as above; and *resourcing adequacy and efficiency*. Please see the article in the VLC on Managing the Department – Process Management, for more information on Quality Assurance. For resourcing efficiency you could report staff efficiency i.e. the time spent on assurance activity versus that on training, admin etc.; number of qualified staff; turnover; sickness rates; vacancy levels; co-sourcing days etc. Another aspect to show is that you've covered emerging external and internal risks and 'hot topics' to your industry or in risk management.

If your department has stated it will comply with the *International Standards for the Professional Practice of Internal Auditing**, then your assurance report to the Audit Committee may be a suitable place to document certain requirements within the standards: such as confirming annually the organizational independence of the internal audit activity; the nature of any impairment to independence or objectivity; the results of the quality assurance and improvement program; or the impact of resource limitations.

You must also report periodically on 'the internal audit activity's purpose, authority, responsibility, and performance relative to its plan'. You must also state the impact of non-conformance with the Definition of Internal Auditing, the Code of Ethics, or the *Standards*, where it impacts the overall

scope or operation of the internal audit activity. Also please remember that if you wish to state in your assurance report that you conform with the *International Standards for the Professional Practice of Internal Auditing,* you are only allowed to do so if the results of the quality assurance and improvement program support this statement.

2) Other Assurance

Assurance is provided to more than just the Audit Committee. *Have you assessed your other stakeholders and their assurance needs?* These stakeholders could include divisional senior management; risk owners / 2nd line of defence senior managers; external audit; pension trustees; and regulators.

For large organisations, I would expect Internal Audit to provide written reports *to divisional senior management* at least every six months and probably quarterly. Some of the things to consider including would be brief results of audit work undertaken; work planned; the status of outstanding issues; and risks / issues accepted for review. Again, you could consider adding an executive summary and even an opinion. An important point to remember is that this report and the meeting to discuss it are key opportunities to inform and influence, plus there should be nothing relevant appearing in the Audit Committee report which would come as a surprise to them as is wasn't in their report.

For *senior management in Risk, Compliance and other 2nd line of defence areas* in large organisations, a periodic written report and meeting to discuss it are also useful. This report would cut the same organisational information by risk category instead of division. This helps produce a 'belt and braces' approach to influencing on audit issues identified, firstly by influencing the manager directly responsible in the business, and secondly by influencing the manager overseeing the risk impacted by the control issue. An example would be an issue which could lead to material fraud being reported to both divisional management and the Head of Financial Crime.

For more information on working with other assurance providers, please see the Virtual Learning Centre.

*For the full text of the Standards, please see http://www.iia.org.uk/