Chartered Institute of
Internal Auditors

Top tips for internal auditors

Writing about risk

Whether you're writing an audit report, advising a client about a risk register or simply mapping out a flow-chart of a business' risks and responses, it makes sense to be clear about what the risk is. This seems obvious, but it's all too easy to get caught up in detailing everything that could go wrong – without considering whether it's a risk or a failed control.

The IIA's International Standards define a risk as 'the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of likelihood and impact.' So how can you make sure you communicate risks as accurately and clearly as possible?

- Understand the business' objectives. Knowing what makes the difference between success and failure of a business is essential. If you're auditing a business function, check that its objectives marry with the overall business objectives.

- List everything that could prevent the achievement of business objectives in the area you're auditing. Then look at how the business' senior management expresses and assesses risk – after all, it's first line of defence's job, not yours! By comparing your list to management's, you'll get a feel for how well the risk management process is working.

- Make sure you've understood *how* the business has assessed its risks – has anyone understated or exaggerated the impact or likelihood of certain risks? In the former case, the risk rating will be misleadingly low. In the latter case, being fearful of *all* risk will stop a business growing. Quantifying the risk means it is possible to set risk tolerances to assess the effectiveness of controls – are risks being held within their tolerance level?

- Beware of one-word risks on risk registers – yes, 'staff', 'cash' and 'property' are all things that have risks attached, but they're not risks in themselves. Make sure the first line – management – is explicit and specific in naming risks.

- How many of the 'risks' are truly risks, and how many are merely failed controls? For instance, if you're looking at a payments area, one risk is financial loss to the business. However, staff failing to authorise payments correctly is not a risk – it's a failed control.

- A good way to do this is to ask, 'So what?' of everything listed as a risk. So what if staff don't authorise payments correctly? So what if new staff don't receive training when they start? So what if the monthly report doesn't go out? Unless you can explain how this specific failure leads to regulatory, reputational or financial risk, you won't be able to make a case for it as a business risk.

- There may be more specialised types of risk – for instance, such as liquidity or credit risk in financial organisations – but if you can link a risk to one of the three types named above, you definitely have a risk. Say so.

- When you describe a finding or issue in a report, include management's quantification of the risk. This may be easier to do with financial loss or regulatory censure (and fines) than a risk that damages the organisation's reputation, but painting a picture for readers will help them grasp the consequences more fully.

- Not all your readers will care whether a risk is inherent or residual, but your job is to make it clear whether the risk in question is unmitigated – therefore inherent – or residual, thanks to adequate controls. In the former case, the risk description needs to set out clearly the consequences of not putting adequate, effective controls in place – of leaving it inherent. In the latter case, your credibility with the business will improve if you show that you understand the mitigating controls in place and have measured their adequacy and effectiveness correctly. The business is then much more likely to take corrective action, if needed, to improve the existing controls and reduce even further the residual risk.

www.iia.org.uk
Chartered Institute of Internal Auditors
13 Abbeville Mews, 88 Clapham Park Road, London SW4 7BX
tel 020 74980101 fax 020 7978 2492 email technical@iia.org.uk