Strategic RISK

Inherent risk ranking: Why bother?

November 2009

Richard Archer explores the concept of inherent risk ranking, and asks if it's worth the effort

Inherent risk ranking (ranking risks assuming no controls) is a core part of the risk management process for many organisations, particularly in the public sector. Furthermore, it is defined in the new British Risk Management Standard, BS31100, and so is likely to become more widespread. However, is inherent risk ranking worth the effort?

I ask this question first because the conceptual nature of inherent risk ranking can be confusing – are people actually able to give accurate inherent risk rankings? Second, if people are able to rank inherent risk accurately, are the benefits sufficient? Given that risk managers need to demonstrate the benefits from their work, it is important that each part of the risk management process delivers sufficient value.

Many private sector organisations have come to the decision not to carry out inherent risk ranking. As a risk manager from a major food company puts it, 'We do not see risk ranking as sufficiently value added. We would rather people pragmatically focus on current risk ranking and action planning.'

Can inherent risk ranking be accurately carried out?

Ranking risks assuming no controls can be a cognitively challenging. What is considered a control or not can be unclear. First, people are faced with the question, what does 'no controls' actually mean? Does it mean: no checks on recruitment? No front door? No management supervision? In addition, it can be unclear whether external factors that influence the level of inherent risk should be assumed away. For example, should the services of the fire and rescue services be assumed away for the inherent ranking of fire risk?

If people struggle with inherent risk ranking, the result will be inconstant ranking, which can lead to poor decision making. Also, if people inherently rank nearly all risks as high, this does not take the analysis forward.

Ray Butler, the former risk management adviser of the Highways Agency, agrees that inherent risk rankings can be challenging for some risks. He says, 'Some controls are so much part of the landscape and taken for granted that it's very difficult to imagine how things would be in their absence.'

David Clayton, head of corporate risk management at the Department of Work and Pensions (DWP), states that in his experience people are able to understand the theoretical concept of inherent risk but sees that inherent risk ranking has the potential to cause confusion and frustrate conversations at risk assessment sessions. To prevent this confusion, he encourages people to rank inherently only after ranking with existing controls.

As Clayton explains: 'Personally, I think it is easier for people to consider/assess residual exposure (with controls) first since this reflects the reality of here and now taking into account knowledge of existing controls. Once the residual rating is agreed it is then easier to work backwards and pose the question as "What do you consider the level of exposure would be if controls were not operating/non-existent?" This may appear "back to front" in terms of the recognised process flow – but for me this will probably deliver a more accurate assessment. After all, mitigation action should be driven by the level of residual exposure versus appetite.'

What are the benefits of inherent risk ranking?

There are several possible benefits.

• Understanding the 'worst case scenario' The most common reason for inherent risk ranking is to determine the worst case scenario for risk exposure. This information can be used to guide the level of insurance purchased. However, assuming all controls fail simultaneously is a very heroic assumption, and a total inherent risk profile is only useful if a large number of controls could fail simultaneously. While there are examples of multiple control failures for individual risks, it would defy probability for all controls to fail across an organisation.

Some organisations take the view that they will rank risks twice only, to minimise the time required to carry out a risk assessment. In such cases, the risk manager has the decision to remove either residual (with controls) or target risk ranking (after additional actions). Residual ranking will usually be the most important of the three rankings, as it shows the actual level of risk faced.

Target risk ranking, however, can also be seen as important, as it demonstrates whether additional actions are sufficient to manage intolerable risks. Certainly in project risk assessment, knowing the target risk ranking is crucial – in projects the current situation is often unacceptable at the start as few controls might be in place. If risk managers want people to risk rank inherently in addition to the other two, then ranking three times is required.

• Controls improvement and assurance Inherent risk ranking helps management understand better the effectiveness of controls and encourages discussion as to whether existing control strategies are correct and optimal. Butler says that inherent risk is important to ensure that 'the current risk exposure is not over-controlling and therefore wasting resources'.

Clayton sees the greatest benefits of inherent risk ranking being with controls. He says, 'I see inherent rankings as having real value in the "control environment" rather than the "risk assessment arena" – in that they help to focus management attention on the need to investigate and understand the control environment. Significant difference between the inherent and the

residual ratings highlights dependency on existing controls – and introduces the need for management to be satisfied/gain assurance that the controls are:

- the right ones

- proportionate in relation to exposure reduction (too many/too costly/are there cheaper alternatives?)

- operating as intended (will controls actually reduce exposure?)

- being complied with (are people actually operating the controls).'

• Risk-based auditing Inherent risk ranking is often used to make audit programmes risk-based. Risk based audits can focus on verifying the effectiveness of the controls of risks with a high inherent ranking. However, a problem with such an approach is that all controls for risks with a high inherent risk-ranking are verified, even if controls are not important to the management of the risk, which is wasteful.

Ideally, audit should place greatest focus on the controls which are key, which are those controls which, if were absent or ineffective, would cause the risk to be residually ranked (after controls) high. Key controls are important as the loss of just a single key control (without the requirement for multiple failures) results in the risk becoming high.

Although stating the effectiveness (weak to strong) of the controls can help guide audit, the effectiveness rating does not inform audit whether the control is key. For the development of risk-based audit programmes, an important question is whether it is better to spend time inherently risk ranking or directly identifying which controls are key (and to be verified by audit).

• Improving residual risk ranking Inherent risk ranking can be used to check the quality of residual (with controls) risk ranking. If the inherent risk ranking and controls listed are not consistent with the residual risk ranking, then the risk manager has a means for identifying incorrect rankings. Although a useful check, this benefit is not generally regarded as sufficient, by itself, to warrant inherent risk ranking. If residual risks are ranked first, like Clayton suggests, then this check is not an option.

• Compliance with risk standards Inherent risk ranking is not generally required for compliance with risk management standards. Most risk management standards are for guidance only and do not have strict requirements for compliance.

For example, BS31100 states that: ‘'Risk analysis should be an iterative process, being repeated as more data becomes available. It may take into account the inherent risk, the controls in place and how well these mitigate the risk, and be undertaken in accordance with the risk criteria.'

The key word here is ‘may’. Organisations can rank with other options, ie residual risk ranking and target risk ranking (after additional actions), without being non-compliant.

In conclusion

Risk managers must ask themselves whether inherent risk ranking is sufficiently value adding for their organisations. In understanding whether inherent risk ranking is worth it, it is important to consider not only if it has benefits, but whether effort is better placed elsewhere. Risk managers should be mindful that time ranking risks inherently is time that is not spent elsewhere, such as action planning.

It appears that the cognitive challenges of inherent risk ranking can be managed, such as through the ranking of residual (with controls) risk first. Risk managers should, however, be aware of the potential pitfalls and provide direction to people as required.

If risk managers wish to rank risks inherently, they should look beyond just using inherent risk ranking to indicate the degree to which controls reduce the level of exposure. Clayton says, 'Perhaps other organisations could use inherent risk ranking – but that the value/benefits are more comprehensible when viewed from the control rather than the risk assessment angle.' Butler agrees. 'You need inherent risk to drive cost-benefit analysis of existing controls and ensuring that they are appropriate to get the exposure right.'

If Risk Managers want to mandate inherent risk ranking in addition to residual and target risk ranking, they will be asking for three rankings. They should be sure that the benefits of improved assessment of controls are worth the extra effort and associated potential push-back from staff. Risk managers should also be aware of the dangers of dropping target risk ranking to make time for inherent risk ranking.

Postscript :

Richard Archer is a senior consultant with DNV, Tel +44 (0)207 357 6080. All contributors are expressing a personal opinion