A Fool with a Tool Is Still a Fool

David Hillson

Software tools can serve a useful purpose in helping us to manage large amounts of risk data with speed and consistency, but we need to be careful to keep them in their right place – as servants of the risk management process and not its master.

The risk management process produces large amounts of data that require careful management in order to support proper analysis, reporting, decision-making and action. The process is also iterative, because of the need to compare current risk exposure with previous positions, supporting use of metrics and trend analysis.

This means that any organisation serious about managing risk needs to think carefully about how to provide the right level of infrastructure to support the risk process and allow efficient storage, analysis and reporting of risk data. Too much infrastructure can create a bureaucratic overhead that wastes time and effort, costs money and discourages use of the risk process. Too little infrastructure support can, however, make it hard to implement the risk process efficiently. The level of infrastructure should, therefore, be chosen carefully to reach the Goldilocks level where the amount of support is 'just right'.

Implementing an infrastructure for risk management might include choosing which techniques to apply within the risk process, allocating resources for risk management, providing training in risk knowledge and skills, developing risk procedures which integrate with other business processes, producing templates for various elements of the risk process and considering the need for support from external risk specialists. However, for most people, 'infrastructure' is synonymous with software tools.

There is no doubt that software tools can serve a useful purpose in helping us to manage large amounts of risk data with speed and consistency, as well as producing good quality outputs. At the same time, we need to keep risk tools in their right place – as servants of the risk process and not its master. It is common for an organisation to invest heavily in a particular risk software package, mandating its use across the business, only to find that staff are so busy maintaining the tool that they are neglecting the actual management of risk. This is like buying a new horse, but spending so much time feeding and grooming it that you never ride it.

Make or buy?

Perhaps the biggest question is where to find a risk software tool that will be right for the needs of the organisation. Many commercial proprietary software tools are available on the market to support different elements of the risk management process. It is also possible to develop bespoke tools for specific applications. The first question is therefore the "make or buy" decision, and lots of organisations seem unsure over this most basic choice.

Organisations starting out in risk management often decide to develop their own simple risk tools, with the aim of migrating to something more sophisticated later on. But perhaps that is a false economy and it would be better to invest immediately in a software package that can grow with the business. A decision to develop bespoke tools should be taken with care, to avoid spending excessive time and resources on the task. Indeed, organisations who have gone down this route frequently find that it is not as easy as it first appears to "just develop a quick risk spreadsheet". Careful specification of the requirement is essential to avoid gold-plating.

It is also common for bespoke tools to contain hidden weaknesses or errors, or to need manual intervention in data manipulation. Problems frequently arise with configuration control, with multiple copies of spreadsheets or databases proliferating around the organisation, all containing slightly different data.

Updating risk data and maintaining history can also be particularly challenging. And combining data from several spreadsheets or databases in order to generate an overview of risk exposure across the business or across a programme of projects relies on a level of data consistency that is usually absent.

As a result of these and other shortcomings, the development of bespoke tools is not usually the best option, despite the initial attractiveness. Most organisations eventually opt for a proprietary risk tool, which raises the question of how to choose from the many on offer.

How to choose?

When making the decision which proprietary software risk tool to buy, you get what you pay for, and it is your responsibility to ensure that whatever you buy will meet your needs. So how do you choose? It is important to avoid implementation of complex systems whose functionality and cost significantly exceed the requirements of the risk process they are intended to support. On the other hand, a tool which is too simple or lacking in essential functionality will just frustrate people and not help them do what needs to be done.
The following are key issues when selecting a commercial software tool:

- Decide the requirement first, then select the appropriate tool functionality to meet that requirement.
- Consider developing an approved requirement specification with weighted selection criteria against which competing tools can be assessed, dividing requirements into categories of must-have, should-have, could-have, won't-have (the so-called MoSCoW approach to requirement categorisation).
- Identify the required user base for the tool, and ensure that this can be supported, for example single-users or concurrent distributed multiple users, co-located or geographically dispersed, different levels of user security access, etc.
- Consult widely with expected users asking them to define specifically what they need from the tool, using the MoSCoW criteria.
- Ensure that the selected tool supports the organisation's existing risk management process, and do not allow the process to become tool-driven.
- Consider integration issues with other existing tools and processes, including data transfer, data formatting conventions, update frequencies, etc.
- Assess the standard set of reports and outputs provided by the tool, as well as the option for production of bespoke reports, to ensure that required report formats can be generated automatically, and that additional *ad hoc* flexible reporting is also possible.
- Consider training needs, and ensure that training is available from the vendor or other recognised expert providers.
- Consider maintenance needs, and ensure the vendor provides ongoing support in a timely and cost-effective manner.
- Ensure scalability, so that the tool can support risk management at various levels across the organisation, including high level and detailed implementations, or projects ranging in size from very small to mega-large.
- Build in growth potential, so that the system can grow with possible changes in the requirement or the business.

These basic criteria should form the foundation of a selection process which can be used to screen the available risk tools, forming a short list of a few tools to be considered in more depth. You can then invite the short listed vendors to a competitive 'beauty parade' or 'shoot-off', where the organisation addresses implementation issues in more detail.

This should include trial installations where the standard functionality can be tested using actual risk data from the organisation (either live or archived, and sanitised where necessary to protect commercial confidentiality), to ensure that the reality lives up to the vendor's sales pitch.

It is notable that the selection criteria discussed above do not mention price or cost. An organisation which is considering buying a commercial risk tool should set a budget, and affordability is a key parameter of the decision, but cost should not be the driving consideration.

Ts or Cs?

Organisations wishing to implement risk management effectively will probably start by considering the three Ts: techniques, tools and training. While these are undeniably part of what is needed to support effective risk management, they are not enough – they are necessary but not sufficient. Any approach to managing risk will involve using a range of techniques, and many of them require tools to support them.

The specialised nature of risk techniques and tools is likely to raise the need for training so that staff can use them properly. But these three elements alone will not make risk management effective, as amply shown by the common experience of many organisations who thought they would. In addition to these three Ts, a number of other critical success factors must also be present, notably the three Cs:

- **Culture.** The organisation must demonstrate a set of values, attitudes and behaviours that respond appropriately to risk, taking the right levels of risk where necessary, and making risk-aware decisions at all levels.

- **Competence.** All staff need to possess the knowledge, skills and experience to enable them to recognise and manage risk at their level of responsibility, and must only act within their boundaries of competence.
- **Commitment.** Risk information must be used to inform decisions and actions across the organisation, and everyone should be committed to appraise risk exposure honestly and to respond appropriately.

In the final analysis, we must accept that a mere tool cannot guarantee effective risk management, however good it may be. All the functionality in the world can never substitute for the ability (or inability) of the user. Possessing a copy of Microsoft Word will not make you a novelist, and owning a power drill does not mean you can build a wardrobe. In the same way, use of a risk tool does not guarantee the ability to manage risk. This is summed up in the proverb: "A fool with a tool is still a fool".

Instead, we need to develop a risk-aware culture and risk-competent people within the organisation at all levels, together with the commitment to use risk information to make appropriate decisions and take right actions. Where the three Cs exist, risk management will be effective in creating significant value for the business, and tools will add efficiency to that effectiveness.

David Hillson FIRM is Director, Risk Doctor & Partners.

david@risk-doctor.com
www.risk-doctor.com

Information Risk is a subject option in the IRM International Diploma. It can also be taken as a specialist course. For more information, see www.theirm.org/Qualifications/dipStructure.html