



A fool with a tool is still a fool

By David Hillson, The Risk Doctor

Servant or 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, resulting in the need to be able to compare current risk exposure with the previous position, supporting use of metrics and trend analysis. This means that any organization 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 in order to reach the 'Goldilocks level' where the amount of support provided 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 both 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. However we need to be careful to keep risk tools in their right place – as servants of the risk process and not its master.

It is common for an organization 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 your organization. Many commercial, proprietary software tools are available on the market to support

different elements of the risk management process, and it is also possible to develop bespoke tools for specific applications. The first question is therefore the 'make or buy' decision, and lots of organizations seem unsure over this most basic choice. There are scores of competing products, all claiming to meet your needs. Or should you develop your own tool in-house, based on common office software spreadsheets and databases?

Organizations 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 significant time and resources on the task. Indeed organizations that 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 organization, all containing slightly different data. Updating risk data and maintaining history can 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 its initial attractiveness as a 'quick and easy' solution. Instead, most organizations eventually opt for a proprietary risk tool, which raises the question of how to choose from the many on offer.

How to choose?

When the decision is made to purchase a proprietary software risk tool, it is important to remember the ancient warning of 'caveat emptor' – let the buyer beware. 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 exceeds the requirements of the risk process it is intended to support. On the other hand a tool that is too simple or lacking in essential functionality will just frustrate people and not help them do what needs to be done.

The following key issues should be addressed when selecting a commercial software tool:

- Decide the requirement first, then select the appropriate tool functionality to meet that requirement
- Develop a 'requirement specification' with weighted selection criteria against which competing tools can be assessed, using the MoSCoW approach to requirement categorisation (Must-have, Should-have, Could-have, Won't-have)
- Identify the required user base and ensure that this can be supported. Ask users about their MoSCoW criteria
- Ensure that the selected tool supports the organization'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 tool training is available from the vendor or other recognised expert training providers
- Consider maintenance needs, and ensure that ongoing support is provided by the vendor in a timely and cost-effective manner
- Ensure scalability, so that the tool can support risk management at various levels across the organisation, including both high-level and detailed implementations, or projects ranging in size from very small to mega-large.
- Build in growth potential so that tool can grow with possible changes in the requirement or the business

These basic criteria should form the foundation of a selection process that can be used to screen the available risk tools, forming a short-list of a few tools to be considered in more depth. The short-listed vendors can then be invited to a competitive 'beauty parade' or 'shoot-off', where the organization addresses implementation issues in more detail. This should include trial installations where the standard functionality can be tested using actual risk data from the organization (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. Of course an organization that is considering buying a commercial risk tool should set a budget for this, and affordability is a key parameter of the decision. But cost should not be the driving consideration.



About the author

Known globally as *The Risk Doctor*, Dr David Hillson PMP HonFAPM FIRM is director of Risk Doctor & Partners (www.risk-doctor.com). David is recognised internationally as a leading thinker and expert practitioner in risk management at both strategic and project levels, and he writes and speaks widely on the topic. He is active in the Project Management Institute (PMI) and received the PMI Distinguished Contribution Award for his work in developing risk management over many years. He is also an Hon. Fellow of the UK Association for Project Management (APM), and a Fellow of the Institute of Risk Management (IRM).

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

Ts or Cs?

Organizations wishing to implement risk management effectively will probably start by considering the Three T's: 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.

Of course any approach to managing risk will involve using a range of techniques, and many of these 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 T's, there are a number of other critical success factors which must be present, notably the Three C's:

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, from the board room to the shop floor, 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 that tool 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'.

Giving a software package to someone who doesn't know what they are doing simply allows them to implement their foolishness more quickly and efficiently. Instead, we need to develop a risk-aware culture and risk-competent people within the organization at all levels, together with the commitment to use risk information to make appropriate decisions and take right actions. Where the Three C's exist, risk management will be effective in creating significant value for the business, and tools will add efficiency to that effectiveness.

