SPONSORED FEATURE **RISK MANAGEMENT**

Leaving risk to chance

Risk is recognised as a hot business topic, but is still not managed as well as it could be, finance directors tell a *CFO World* survey

Risk is currently the hottest topic in business. High-profile scandals such as software glitches locking customers out of their bank accounts, the Gulf of Mexico oil spill, price fixing fines for anti-competitive behaviour and product recalls all remind us that doing business in the modern world can be dauntingly complex and fraught with risk.

As governments have reacted with tighter rules and new regulations, risk, and the effective management of risks, has moved ever higher on board agendas. Regardless of which sector you work in, episodes like these serve as a reminder that a corporate body has to be extremely vigilant when looking for and managing the risks to business. Unchecked, such incidents can at best damage the reputation of your enterprise, and at worst threaten its very survival.

In recent years new approaches to risk management have evolved at an astonishing rate and many businesses have responded with more sophisticated systems and an overhaul in their methods for addressing risk.

But new research reveals that this attitude is not entirely widespread, and that managing the uncertainties involved in business via an integrated risk management framework is not necessarily a universal approach, nor has the adoption and effective use of the latest governance, risk and compliance (GRC) software tools been comprehensive.

Indeed, there appears to be significant obstacles for organisations to effectively tackle risk management including problems grasping its finer points as an issue, fears about the cost of applying an integrated risk management framework and the understanding of the commercial benefits in full.

David Walter, general manager for GRC at software specialists RSA, says: "What's so difficult for organisations is that they grow in complexity. But we only have limited resources for managing our top risks. So, how do we identify the important ones? Everyone's trying to get their risks and programmes to the top of the list. It's important to understand which ones need attention."

The good news

Despite the concerns there is some good news. Recent research conducted by *CFO World* revealed that having an integrated risk management framework (IRMF) is a popular option. A hefty 71 percent of CFOs questioned said their organisations had such a structure in place. That left almost a third with no IRMF, a substantial number given the complexities of managing risks in these uncertain times. Those who did not were ready to reveal what they were missing out on.

When asked what the main issues were that resulted from the absence of an integrated framework most CFOs indicated two key problems. They had no "single view" of the risk in their organisations and suffered from an "inability" to measure the effectiveness of the risk management measures they did have in place. When this group was asked whether they would benefit from an integrated approach to risk management not a single respondent said no.

Of course, understanding the nature of an "integrated" approach is critical. Without it, it's impossible to grasp the benefits that can be had from implementing one. Past practice has mostly seen risk management consigned to silos. To put it another way, it's managed through units that rarely if ever talk to each other to combine their efforts. A single organisation would therefore have multiple views of risk management, completed using different measures all creating a multitude of documents making it difficult to generate a whole picture of the risk profile of an organisation.

An integrated framework attempts to do something else: it aims to offer a single, simple but well-founded overview of the risk position of an organisation. According to a paper published last year by IT analyst Gartner, this kind of approach to risk should support a "company's ability to increase risk awareness and accountability and improve business decision making."

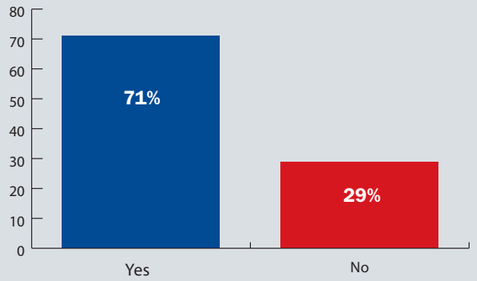
> How do we identify the top risks? It's important to understand which ones need attention
>
> DAVID WALTER, RSA

An integrated approach may break the risks into types of risk – strategic, preventable operational risks and external risks. These may overlap (giving a broad idea of the kind of risks that need to be managed) but the idea is to assess and standardise these elements so they can be compared. In a traditional approach to risk that wouldn't normally be the case. A change in a strategic risk, such as an advance in technology, is difficult to

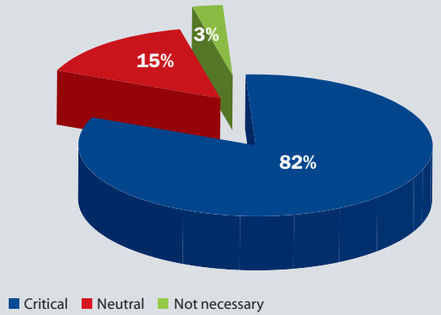
▸▸

SPONSORED FEATURE **RISK MANAGEMENT**

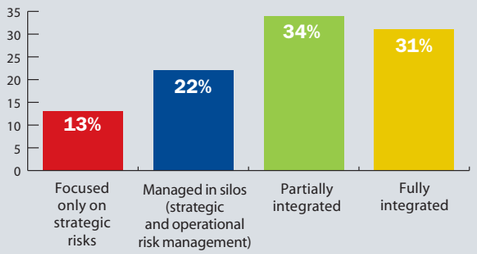
Does your organisation have an integrated risk management framework?



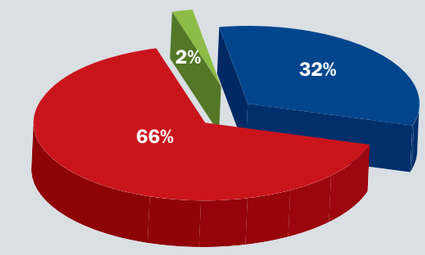
How important is it for your organisation to control strategic and operational risks?



How would you describe your current approach to risk management and systems?



Do you understand how an integrated risk management framework functions?



compare with, say, a failure to comply with a piece of financial reporting regulation. But the impact of each can be expressed in a standardised way so they can be set side by side and then evaluated in terms of their relative importance to the business. The result should be a process which manages any number of risks but produces a list of the most significant so that management can target their efforts accordingly.

Paul Cadwallader, a director in the Audit-Advisory practice at Deloitte LLP, says an integrated risk management framework keeps the risk messages "simple" for staff in an organisation.

"If you don't keep it simple you are going to need to employ a lot of experts to manage the risk, which nobody is going to understand and it becomes a bolt-on, on the side of an organisation set in a siloed part of the business," he says.

Knowledge and simplicity

If simplicity is the message it's not one that appears to have landed in all quarters of business. Just one third of finance chiefs who took part in the research said their risk method was "fully integrated". Everyone else said their approach was either narrowly focused on strategic issues, siloed or only partially integrated.

That appeared to tally with the state of knowledge of the area among the respondents. A minority, once again around a third at 32 percent, said they had a "strong understanding" of how an integrated risk management framework operates. Nearly all the other CFOs who took part in the survey said their

TROUBLED WATERS
High -profile failures like the Gulf of Mexico oil spill can have an impact on both reputation and bottom line

understanding was only "moderate". A very small group said they had "little understanding", and this is while a hefty 82 percent say that it was "critical" for their organisations to control strategic and operational risks.

Despite the recent rash of corporate disasters that point to the ever present need for sound risk management, the results suggest that the C-Suite knowledge-base around risk management issues leaves much room to be improved.

It's possible that this knowledge deficit feeds into the fears and worries that circulate around an integrated approach to risk management. The research asked respondents to identify their major concerns from a list of obstacles that could hinder their investment in an integrated approach to risk management. Those taking part were allowed to choose more than one, but the most popular was the potential cost, underscored by half the finance chiefs questioned. The next most important consideration was uncertainty about the benefits that could be achieved.

However, when asked to rank the biggest barriers to achieving an integrated risk management framework, the issue most often nominated was a lack of executive champions, identified by 28 percent of those involved in the study as their top snag. That said, 13 percent identified their technology was their most significant worry because it was not aligned to an integrated way of tackling risk. The next largest groups of respondents elevated the lack of a business case and understanding the cost benefits as their major roadblocks.

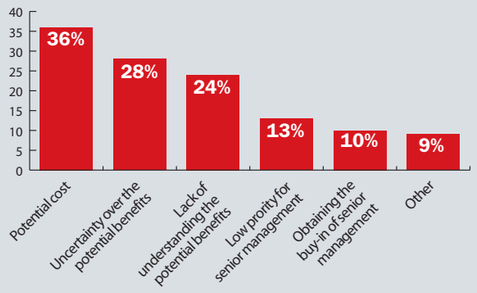
Much of this is closely related to respondents' attitudes to the technology part of getting to grips with risk – a governance, risk and compliance (GRC) tool, or software, which supports an integrated risk management process. When asked to rank factors used in evaluating the potential of GRC software, 34 percent said "ease of use" was the most important but that was closely followed by the next largest group, 22 percent, needing a "rapid return on investment". When asked what actually stopped them from buying GRC technology, the biggest batch, 35 percent, said it was the lack of a business case, while 24 percent lined up behind expense as the largest stumbling block. Interestingly, only 7 percent pointed to complexity of the software as a big turn-off, suggesting

> If you don't keep it simple your are going to need to employ a lot of experts to manage the risk
>
> PAUL CADWALLADER, DELOITTE LLP

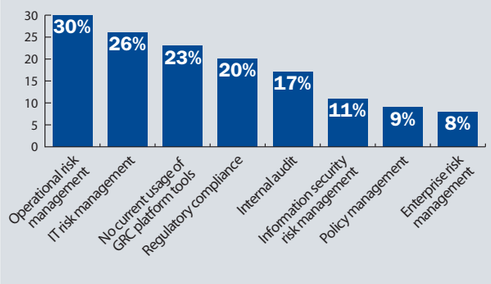
SPONSORED FEATURE **RISK MANAGEMENT**

What are the obstacles to investing in an integrated risk management framework within your organisation?

Cost was considered as the main obstacle to investing in a risk management framework

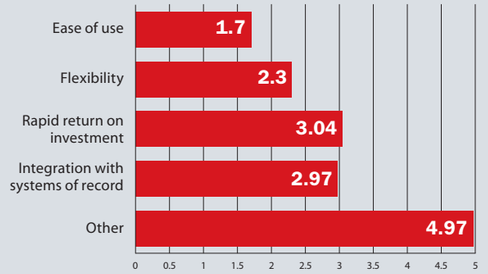


Areas of your business concern for which GRC platform tools have been adopted and deployed



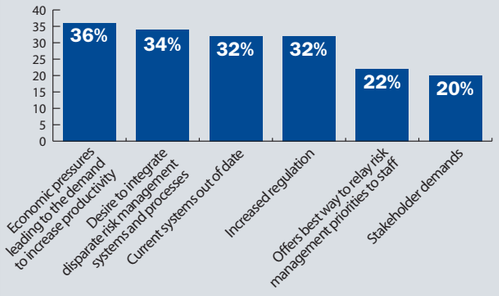
How important are the following factors when evaluating technology to support your company's GRC strategy?

Results based on a mean average where 1=most important and 5=least



What are the internal drivers behind your acquisition of GRC tools?

Respondents were asked to name their top 3 drivers



> The board has to have a holistic view of risk in order to prioritise the money they have to fix the risks that confront them
>
> DAVID WALTER, RSA

respondents were happy to come to terms with the technical demands of GRC technology if only they could win executive backing and some resource to fund a project. Likewise, CFOs questioned mostly seemed happy to grapple with an integrated approach to risk management, if they could be persuaded of the benefits and get the board on-side. In short, if executives are to be persuaded they will need to see the benefits of having a new integrated approach and a new software platform on which it would be managed.

Experts identify two cardinal areas where they say significant improvements can be made with an integrated approach. The first is an improved view of an organisation's risk position, and the second is streamlining how that risk view is reached. Both of those are achieved because an integrated system removes the silos in which compliance (tackling preventable risks) is managed.

Paul Cadwallader of Deloitte says the best way to see how the silos arise is by looking at the classic three lines of defence for managing governance, risk and control. The first line is management who set policy and own/operate controls. The second are the functions like compliance, risk management, health and safety and quality control who guide, support and challenge the first line. The third is internal audit which provides independent assurance of how risk is being managed across the organisation. For Cadwallader though, it is often the second line of defence that is problematic.

"That's where all the silos are built. They'll have their own frameworks, methodologies, reporting lines and terminology, sometimes even their own technology. It's no wonder their boards do not have a single view of risk," he says.

According to Cadwallader, leaving the silos in place means maintaining a "fragmented" risk management framework that is inefficient in terms of process, but fails to offer a single vision that could enable management to approach risk more effectively and improve the day-to-day running of the company. Silos make the job of allocating resources to tackle risk more difficult. RSA's David Walter says: "The board or senior management has to have a holistic view of risk in order to prioritise the money they have to fix the risks that confront them."

CFOs are not unaware of the potential benefits to be had from GRC technology supporting an integrated risk management plan. When asked what they hoped to gain from implementing governance, risk and compliance software, most chose visibility of their organisations' risk as well as efficiency gains from cutting redundant processes, and the ability to improve information gathering for board reporting. It should not be a surprise. Asked about what was driving their search for benefits, among the top reasons was a desire to integrate disparate management systems along with increased regulation and ageing systems. Their top concern, however, was "economic pressure prompting a demand for increased productivity".

Forrester, the technology analysts, highlight the efficiency gains that can be made with integrated governance, risk and compliance in a report, Build the Business Case for a GRC Platform. In Forrester's view there is a general acceleration that takes place, post integration, allowing companies to speed up the review and fixing of policy and controls, quicken the identification of risks and their evaluation, as well as pushing along the actions needed when problems are uncovered.

> With software, boards are better placed to see through the fog of compliance between decision makers and those 'on the ground'
>
> PAUL CADWALLADER, DELOITTE

Deloitte's Cadwallader puts it another way. Once software is in place to enable an integrated risk strategy company boards are better placed to see through what can be described as the "fog" of compliance between the decision makers and those "on the ground" in an organisation. This "fog" is composed of a splintered view of what is happening on compliance and the preventable operational risks. Splinters emanate from inefficient processes housed in silos failing to communicate with each other and potentially using separate bits of technology with little or no integration. Change tack though, put in an integrated framework backed by the right technology, and a company can achieve a single view of their risk position with shared technology using a common vocabulary and methodology. The technology means the whole picture can be shown on an easy to read dashboard highlighting specific areas of concern. "Where a company has a more mature integrated risk programme, they tend talk about a lower number of risks at the board level," says RSA's Walter.