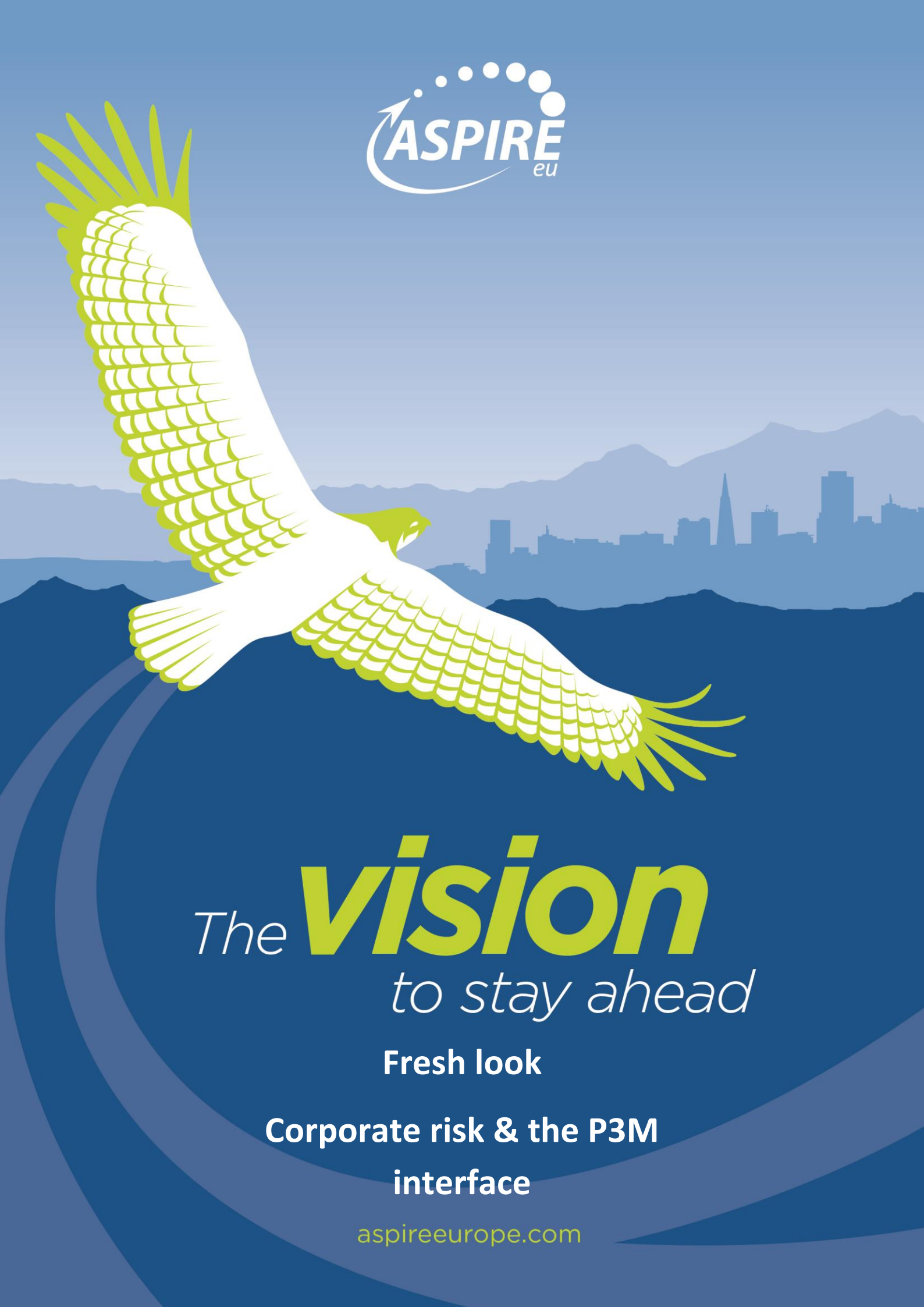

ASPIRE eu
The vision to stay ahead
Fresh look
Corporate risk & the P3M interface
aspireeurope.com

Are you wondering why risk management isn't really having the 'bite' it should in your organisation. Have you got too many projects going wrong?

After delivering over 500 P3M3® assessments we have a pretty clear handle on what makes organisations tick, and more importantly, the things stopping them performing productively.

In this article we take a fresh look at the issue of the corporate risk management environment. One of the most common failings in P3M3® assessments is finding a dysfunctional risk management environment where each element of risk management is operating in isolation from the other elements.

As such, we find projects managing the same risks but describing the risk differently so nobody is able to see the potential dangers from a risk maturing across a number of projects.

The corporate risk and P3M risk processes are invariably disconnected so the overall exposure to risk from the P3M environment is not being tracked, and in fact, it is being lost within a myriad of spreadsheets.

Fresh Look

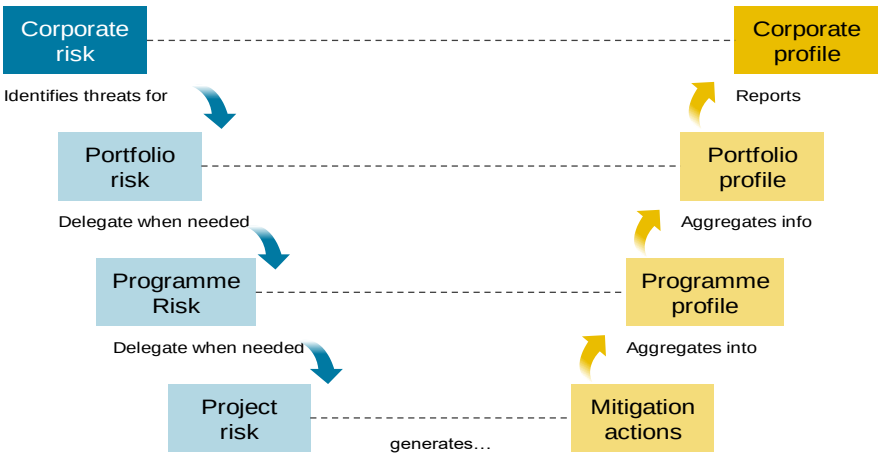
Is a series of articles taking a look at common topics to try to come up with some new ideas and insight into problems that seem to repeat themselves across many organisations.

Occasionally the two processes are bridged by the teams having meetings and exchanging information effectively, but this is people dependant and lacks systemic formality.

In response to this common scenario we have developed a simple model that helps to illustrate how the processes should be married together with corporate risk cascading down through the P3M layers and the mitigating actions managed.

An effective corporate risk environment will be identifying a whole range of threats and trying to understand how they will affect an organisation. Taking a common corporate threat such as cyber security, there is little that can be done to completely remove the threat without disconnecting the organisation from the world, therefore it needs to be managed.

On the left side of the V, the threat is passed to the portfolio office, which mandates that all programmes and projects have a standard threat of cyber-attack so any change they are implementing then considers the potential implications on cyber security, enhancing or reducing it by their actions.



At the programme level they can consider the project outputs being commissioned and the business changes that will be implemented to understand what and where the threat could materialise as a risk.

Brexit is a classic threat within many organisations - that is, a threat causing risks and activity in all the layers

This in turn can be cascaded as a specific risk for individual projects and changes, but the corporate threat of cyber-attack is also considered at the project level as there may be activities the programme is not aware of. In many cases there may be no risk at all, but at least it has been considered by everyone. However, there will also be projects where it does apply where these may not have been considered before and mitigating actions can now be applied.

That takes us to the bottom of the V with the full scale of the threat fully understood and the Corporate layer can see the full exposure to the threat from the P3M environment. They will know what activities are being planned that will create actual risks from the abstract threat of cyber-attack and information linkage.

The right side of the V illustrates the reporting and control to ensure the activities are being controlled with the appropriate level of specialisms and testing. The risk reporting on potential mitigation and costs from the projects will be reported to the programme. Where the information is aggregated in the programme, this reports back to the portfolio along with their own programme specific risk mitigation and costs, in particular, the risks linked to business changes.

All this can then be assembled at the portfolio level and the Corporate risk functions will have a consolidated view on how the P3M world is managing risks linked to this corporate threat and the management activities can be much more focused and pragmatic, thus creating a pyramid out of the information reporting.

We've used cyber security as an example, but depending on your environment, health and safety, resource availability, or any other threats can be used to consider the possibilities.

This simple model addresses the vast majority of issues that organisations face when integrating corporate and P3M risk, unfortunately the simplicity is lost by failing to deal with the integration, or implementing complex tools which create an industry of information gathering and little in the way of improved risk management.

In one of the more bizarre scenarios we found, the corporate risk team regarded the programmes as risks even though all the programmes were in place to address corporate risks.

Fresh look tips

So, having taken a fresh look at the challenge, here are some suggestions on how to improve:

1. Manage risks in the right place, the same threat can be manifesting itself in many different ways and places and having clear ownership and oversight enables better management, a recent example being the Carillion collapse
2. Maintain focus by tracking threats to the organisations strategic objectives, not every little thing that could go wrong

3. Risk management should be integrated with a common vocabulary and syntax in both environments. This should be achieved through portfolio and programme risk management Strategies
4. The corporate risk function should ensure the corporate threats are cascaded through the P3M portfolio, not managed in isolation as per our example
5. Programmes and projects often exist to reduce a corporate risk, yet this is rarely traceable through the documentation
6. The activities within the P3M portfolio will be increasing or reducing the threat level and the corporate risks, these actions should be traceable for reporting and profiling

Article written by: Rod Sowden

Rod Sowden is the managing director of Aspire Europe and an experienced programme management registered consultant with a number of successful consulting and delivery assignments behind him that have left organisations with sustainable change.

Rod has been a pioneer of Managing Successful Programmes (MSP®), having been involved since the launch in 1999 he was appointed lead author by the OGC for the 2007 version and 2011 refresh. He is also the Cabinet Office P3M3 lead author. Rod as subsequently written survival guides for the business change managers, senior responsible owners and programme managers as well as having numerous articles published in his expert field.