The Institute of Internal Auditors
Australia

Dear Q&A

Why is there a need for both an assurance map and a risk register?

Answer

An assurance map and a risk register are complementary, and the existence of a useful risk register will reduce the amount of material within the assurance map. Neither document has a prescribed format and you should be careful about making either of them too much work. Both documents can be developed at multiple levels of detail, so they can become unwieldy if you are not careful.

An assurance map is designed to show the importance of control processes in an activity and the source and quality of assurances in relation to those activities. Remembering that assurance is in relation to the objectives of the process, it will consider organisational exposure in the event of failure to achieve objectives. Sometimes it will consider the assessed quality of the control design where there is some basis for this assessment and then the quality of the review processes in the other lines. An assurance map will not necessarily detail all these components but will provide a high-level picture (map) of them. Initially, it may go no further than indicating which assurance activities or entities conduct the reviews. Over time a view of the quality of each assurance activity will develop to fill out the picture. Importantly, an assurance map should cover the whole area of interest. Only as much detail as can be kept current should be included.

A risk register is intended to record information about risks in support of decision-making. While it is important to document the controls that are managing individual risks, this need not be within the risk register. If the information about controls will be used on an ongoing basis for management of risk, then placing it in the risk register may be valuable. The purpose of risk assessments is to inform operational strategies, resource allocation and other decisions. The organisation will need to document the controls it depends on to manage risks, but it will not necessarily find the risk register the most convenient place to do this.

Some organisations find that ‘managed’ risks begin to make the risk register too big. Some even remove ‘manage’ risks from the register – this is poor practice but understandable. Managers need to pay attention to more dynamic issues, but still must not forget what they believe has been addressed. The risk register reporting should be designed in a way that draws attention to the decisions required. An agreed response to a risk that has not been finalised is like an agreed internal audit recommendation that is not yet complete. There is much to be said for using the same mechanism to deal with them.

Stable control processes in support of operational objectives may be best managed within an obligations register. In this context an obligation is not only something externally imposed, but also something voluntarily assumed. An obligations register is an important part of a formal compliance program and the quality of the compliance program will be reflected in the assurance map.

So, we now have four documents to think about:

1. The assurance map giving a picture of the sources and quality of assurance.
2. The risk register informing organisational decision-making.
3. The outstanding actions register tracking risk responses that are yet to be finalised.
4. An obligations register which incorporates a stable control process in support of organisational obligations – both imposed and assumed.

It is not useful to make any single document do all these tasks – the four sets of tasks are complementary but are distinct and need their own form of documentation.

Need an answer? Send your questions through to IAassist@iia.org.au