



UNIT-16

Reviewing and Enhancing a Risk Management Framework

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Reviewing a risk management framework
- ✓ Enhancing a risk management framework

Reviewing a Risk Management Framework



What is it?

Reviewing a risk management framework is different to reviewing risks and their associated controls for effectiveness. The latter is a subset of the former as, by obtaining assurance on the effectiveness of the practices in place to manage specific risks, an organisation can be satisfied that at least part of its risk management framework is operating effectively. This review activity would then be coupled with a review of additional components of the risk management framework to ensure its overall effectiveness.

Why do it?

The aim of reviewing the risk management framework is to ensure that appropriate framework enhancements are occurring when and as needed. It is important to be confident in the effectiveness and efficiency of the risk management framework, as it provides the structure within which all risks are managed.

How to review the risk management framework

When reviewing the framework, particular attention should be paid to whether the framework has been appropriately customised and is operating in a manner that illustrates that:

- risks are being effectively identified and appropriately analysed
- this leads to adequate and appropriate risk management and control
- there is effective review by management and executives to detect changes in risks and controls.

Reviewing a Risk Management Framework

There are several approaches available to help organisations effectively review their frameworks, including reviewing the framework against:

- Risk management process components
- Risk management maturity models.

The factors to consider when choosing the appropriate approach include:

- the maturity level of the risk management, as determined through any previous maturity assessments
- the number of planned risk management improvement initiatives currently being undertaken / recently having been undertaken
- the findings from previous risk management framework reviews
- the size and complexity of the organisation
- the number of major risks that have eventuated in that year
- whether the organisation has entered into providing any new services/products
- whether there have been significant organisational changes
- use of implementation partners.

For example, a medium-sized organisation that has been previously assessed as having mature risk management but which had numerous major risks eventuating in the last year would be most likely to undertake a more rigorous review of its risk management framework. The fact that the organisation scored highly in a previous maturity assessment does not outweigh the fact that it has seen many risks eventuate, as this would normally indicate some form of failure in its risk management practices.

It should also be noted that one may choose to use a combination of approaches at different times or alternate the approach used from year to year. For example, it may be appropriate to conduct an annual review of the framework against the process components; however, on a three-yearly basis, it may be useful to conduct a risk management maturity assessment, particularly if over that period a number of risk management improvement initiatives have occurred.

Enhancing a Risk Management Framework

The framework clearly articulates the ‘enhancing a risk management framework’ loop that supports the on-going effectiveness of a risk management framework. Set out below is the diagram provided within that Standard to demonstrate this process.



Why do it?

Continuous improvement and change management is essential for ensuring the on-going relevancy and effectiveness of risk management activities within an organisation. To achieve the greatest benefits from continuous improvement, it must span all risk management framework elements including the process, capability, behaviours, tools and templates, reporting structures, and the practices used to manage actual risks.

How to achieve it?

There is a direct link between the outcomes of review activities and the continual enhancement of the framework. Continuous enhancement is supported and informed by both the review of risks and controls (as outlined in the ‘Implementing the Risk Management Framework’ section) and the review of the risk management framework.

As the continual enhancement of a risk framework includes discrete risk management improvement initiatives, there is understandably a clear link between an organisation’s risk management strategy and the initiatives it wishes to undertake to improve its framework.

The initiatives that are identified during review activities should be prioritised and then included within the risk management strategy and risk plans to ensure that they are appropriately approved

Enhancing a Risk Management Framework

and supported in their implementation. Inclusion of these initiatives in the strategy will also increase accountability for their delivery and should drive a need to measure their value once implemented; this explains the importance of establishing linkages between the various elements of the process outlined in these guidelines.

By continuously improving its risk management framework, an organisation should obtain benefits including:

- Organisational resilience by being more proactive in managing risks as compared to reactive in managing issues
- Better governance through regular reporting which strengthens an organisation's ability to oversee its risks and direct changes in approach where necessary
- Increased accountability through well defined risk management responsibilities against which performance is measured
- Being able to leverage leading risk management practice in its risk management approach.