ORGANISATION OF CERTIFIED RISK MANAGERS

Diploma in Risk Management

Chapter 1.3

Reviewing and Enhancing a Risk Management Framework

Contents

3.1

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.

3.2

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

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.

Bibliography

Some of the most important reference sources which have been consulted during the preparation of this course.

Alarm, 2010. The alarm national performance model for risk management in the public services. Available on http://www.alarm-uk.org/asset.ashx?assetid=bd5d3887-be73-4dfa-ab86-70b0f01f7ff0.

Deloitte, 2013 Exploring strategic risk: A global survey. Available on http://www2.deloitte.com/global/en/pages/governance-risk-and-compliance/articles/exploring-strategic-risk.html.

Ferma, 2003. A risk management standard. Available on http://www.ferma.eu/risk-management/standards/risk-management-standard/

Fraser, J., Simkins, B. J. 2010. Enterprise risk management: Today's leading research and best practices for tomorrow's executives. New Jersey: John Wiley & Sons.

Fraser, J.R.S., Simkins, B.j., Narvaez, K. 2015. Implementing enterprise risk management: Case studies and best practices. New Jersey: John Wiley & Sons.

Hampton, J.J. 2009. Fundamentals of enterprise risk management: How top companies assess risk, manage exposure, and seize opportunity. New York: AMACOM.

HM Treasury, 2004. The orange book: Management of risks – Principles and concepts. Available on https://webcache.googleusercontent.com/search?q=cache:ZL7HkXPNTWAJ:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf+&cd=1&hl=en&ct=clnk&gl=uk&client=firefox-b-ab.

ISO 2009. ISO 31000, Risk management-Principles and guidelines, Geneva

ISO 2009. ISO/IEC. Guide 73, risk management-Vocabulary, Geneva

Taleb, N.N. 2007. The black swan: The impact of highly improbable. New York: Random House.

VAMIA, 2016. Victorian government risk management framework practice guide. Available on https://www.vmia.vic.gov.au/risk/risk-tools/risk-management-guide.

Glossary of Key Terms

The glossary below provides definitions for commonly used risk management terminology.

The ISO 31000:2009 has been used as the primary source of definitions.
Where the Standard does not include a definition of a particular term, other sources have been used.

Communication and consultation
Continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk

Consequence
Outcome of an event impacting objectives

Control
Measure that modifies risk

Control assessment
Systematic review to ensure that controls are still effective and appropriate

Enterprise-Wide Risk Management (ERM)
An integrated approach to assessing and addressing all risks that threaten the achievement of the organisation's strategic objectives; the purpose of ERM is to understand, prioritise, and develop action plans to maximise benefits and mitigate top risks.

Establishing the context
Defining the external and internal parameters to be taken into account when managing risk and setting scope and risk criteria for the risk management policy

Event
Occurrence or change of a particular set of circumstances

Exposure
Extent to which an organisation and/or stakeholder is subject to an event

External context
External environment in which the organisation seeks to achieve its objectives

Frequency
Number of events or outcomes per defined unit of time

Hazard
A source of potential harm

Internal audit
Independent, objective assurance and consulting activity designed to add value and improve an organisation's operations…accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of: (1) Risk management (2) Control, and (3) Governance processes. (IIA Professional Practices
Framework)

Internal context
Internal environment in which the organisation seeks to achieve its objectives

Key control indicator (KCI)
Measures or metrics that demonstrate a change in a specific control's effectiveness

Key performance indicators (KPIs)
Metrics or measures used to monitor changes in business performance in relation to specific business objectives (e.g. volumes of business, revenue etc.)

Key risk Indicators (KRI)
Measures and metrics that relate to a specific risk and demonstrate a change in the likelihood or consequence of the risk occurring

Level of Risk
Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

Likelihood
Chance of something happening

Loss
Any negative consequence or adverse effect, financial or otherwise

Monitoring
Continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected

Probability
Measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

Residual risk
Risk remaining after risk treatment

Review
Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

Risk
Effect of uncertainty on objectives

Risk acceptance
Informed decision to take a particular risk

Risk aggregation
Combination of a number of risks into one risk to develop a more complete understanding of the overall risk

Risk analysis
Process to comprehend the nature of risk and to determine the level of risk

Risk appetite
Amount and type of risk that an organisation is willing to pursue or retain

Risk assessment
Overall process of risk identification, risk analysis and risk evaluation

Risk attitude
Organisation's approach to assess and eventually pursue, retain, take or turn away from risk

Risk aversion
Attitude to turn away from risk

Risk avoidance
Informed decision not to be involved in, or to withdraw from, an activity in order not to be exposed to a particular risk

Risk criteria
Terms of reference against which the significance of risk is evaluated

Risk description
Structured statement of risk usually containing four elements:
sources, events, causes and consequences

Risk evaluation
Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

Risk financing
Form of risk treatment involving contingent arrangements for the provision of funds to meet or modify the financial consequences should they occur

Risk identification
Process of finding, recognising and describing risks

Risk management
Coordinated activities to direct and control an organisation with regard to risk

Risk management audit
Systematic, independent and documented process of obtaining evidence and evaluating it objectively in order to determine the extent to which the risk management framework or any selected part of it is adequate and effective

Risk management framework
Set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk management plan
Scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk

Risk management policy
Statement of the overall intentions and direction of an organisation related to risk management

Risk management process
Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk

Risk matrix (or heat map)
Tool for ranking and displaying risks by defining ranges for consequence and likelihood

Risk mitigation
Measures taken to reduce an undesired consequence

Risk owner
Person or entity with the accountability and authority to manage a risk

Risk perception
Stakeholder's view on risk

Risk profile
Description of any set of risks

Risk reduction
Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk

Risk register
Record of Information about identified risks

Risk reporting
Form of communication intended to inform particular internal or external stakeholders by providing information regarding the current state of risk and its management

Risk retention
Acceptance of the potential benefit of gain, or burden of loss, from a particular risk

Risk severity
A measure of the magnitude of a risk, based on a combination of the likelihood and consequence of a risk

Risk sharing
Form of risk treatment involving the agreed distribution of risk with other parties

Risk source
Element which alone or in combination has the intrinsic potential to give rise to risk

Risk tolerance
Organisation's or stakeholder's readiness to bear the risk, after treatment, in order to achieve its objectives

Risk treatment
Process to modify risk

Stakeholder
Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity