Risk Governance

Driving better identification and management of risk to enable organisations to improve decision making

Risk Governance

Introduction

All organisations face uncertainty on a daily basis. This uncertainty creates the risks that we face whilst trying to achieve our organisation's objectives. Managing these risks is critical as it assists organisations to make better decisions about their strategy and objectives.

At CBO we have aligned to ISO 31000:2018 Risk Management – Guidelines as industry best practice to influence how we approach effective risk management, and the underlying frameworks and processes that need to work together to manage risks across organisations.

The core components of effective risk management are governance risk structure; risk management framework; risk appetite; and risk management processes (set out below).

1. Governance risk structure

Risk management requires effective oversight to ensure that the key decision makers are provided with assurance that the risk management framework, risk appetite and risk management processes are implemented and working as intended. As a result, the key decision makers will understand the risks the organisation faces and can communicate that to key stakeholders and the organisation. A governance risk structure is the structure that an organisation puts in place to evidence and ensure effective oversight over risk management. The governance risk structure should be proportional based on the size and complexity of the organisation.

2. Risk management framework

A risk management framework demonstrates a commitment from the key decision makers to risk management. In documenting your risk management framework, you capture responsibility and accountability, alignment with your strategy and objectives, articulation of your risk appetite(s), guidance on how your organisation identifies, assesses, reports, and communicates risks to the relevant stakeholders of the organisation, and confirmation of who is responsible for the first, second and third line of defence for each risk.

3. Risk appetite

Each organisation should articulate, understand and document their overall risk appetite – which can then be reviewed against each risk it faces. Risk appetite refers to the amount of risk (residual risk; after considering internal controls) that an organisation is willing to accept relative to the organisation's strategic objectives. Each risk should be monitored against the documented risk appetite to ensure that the residual risk is within risk appetite. Risks outside of appetite need to be reported and escalated according to the framework and governance requirements.

4. Risk management process

Risk management includes a structured approach to identifying risks, assessing the inherent risks, analysing internal controls and reporting the residual risks.

The risk management process is a five-step process, derived from ISO best practice.

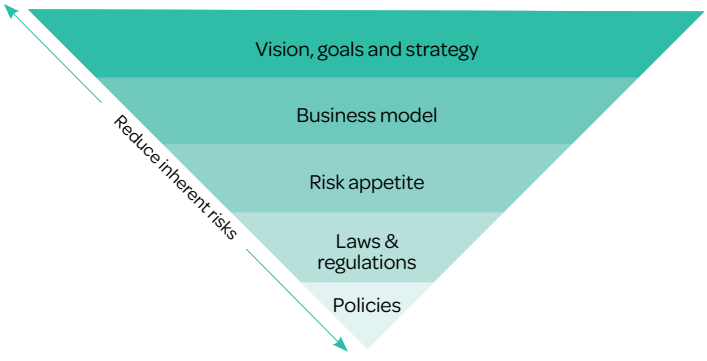
4.1 Identify risks

To identify all the risks that an organisation faces, you need to intimately understand the context to allow you to dismiss the risks that are not applicable to the organisation. By applying the context to a list of potential pre-defined risks, you will be able to eliminate the risks that are not applicable to your organisation, leaving you with list of inherent risks that require further assessment.

4.2 Inherent risk assessment

Inherent risk is the total level of risk that exists before any internal controls are applied, so no risk mitigation is in place. The reality is, that as each organisation is structured differently, the same type of risk may result in a different level of inherent risk for different organisations.
To perform an inherent risk assessment, you need to consider the context, business model, risk appetite, applicable laws and regulations and policies, which in turn helps to reduce or mitigate some of the inherent risks.

Inherent risk before assessment



Inherent risks assessed

4.3 Analyse internal controls

An organisation's internal controls consist of all the processes and procedures that exist to ensure that the organisation adheres to its own risk appetites and policies. The purpose of the internal controls is to reduce or mitigate the risks to an acceptable level within the organisation's risk appetites and/or limits. This step applies the key internal controls to the inherent risks to establish if the controls effectively reduce the inherent risk. The output is an objective assessment of the risks that remain after applying the internal controls.

4.4 Residual risk assessment

The residual risk needs to be reviewed against the organisation's risk appetite and/or limits. If the residual risk is within risk appetite, then there is nothing more to do, other than to report the outcome. If the residual risk is outside the organisation's risk appetite, the organisation needs to consider whether to accept the risk, enhance controls to reduce the risk, amend risk appetite or reconsider the organisation's strategy.

4.5 Reporting

Reporting of the residual risk and whether these risks are within or outside of risk appetite needs to be communicated to the key decision makers and stakeholders to ensure that the organisation can demonstrate effective oversight of the risk management process.

How we can help

We recognise that all organisations operate within different contexts and that risk management frameworks and processes need to be proportionate. Our offering can be customised to your organisation's internal and external context, for example, industry, size, jurisdictions, complexity and/or maturity around risk management.

At CBO we help you understand and navigate your risk governance to help identify your organisation's specific needs and work with you to tailor a bespoke approach. This can vary from a simple 'review' and audit of your existing risk management framework, processes and supporting documentation where we provide you with findings and recommendations, through to a more involved review coupled with the detailed implementation plan required to embed the recommendations needed to 'enhance' your risk management framework and risk processes. Or it may be a that there is a need to start from scratch, in which case we can help you 'develop' your risk management framework and processes, assisting you with embedding these as appropriate and agreed.

We have been supporting many organisations to understand their approach to and execution of risk governance, to help drive better identification and management of risks and ultimately assist organisations to make better decisions. Our team is one of highly experienced and skilled professionals who work collaboratively with our clients to positively influence their approach to risk governance.

If you are interested in learning more about any of the topics raised in this paper, please contact one of our team.

Rudi Le Roux
View profile
07781 103713

Dom Ash
View profile
07839 747369

Philip Smith
View profile
07781 128208

Supporting businesses with unparalleled value for money and quality of service.
We would be delighted to discuss our experience and
insights in more detail with you over a coffee.

CBO Projects
The Albany
South Esplanade
St Peter Port
Guernsey GY1 4AQ

coffee@cboprojects.com

+44 (0)1481 729161