Self-assessment risk analysis

Gunn & Twynmore

Quickscan

June 15, 2015

Schipholweg 103
2316 XC, Leiden,
The Netherlands
Phone: 06-28986660
E-Mail: gt@gunntwynmore.com
Web: www.gunntwynmore.com

How to use this Quick Scan

This Quick Scan is meant for a quick internal assessment of your business. It is not a full analysis of your company and we advise to seek professional advice in addition to the Quick Scan. The aim of the Quick Scan is to give management a quick way of analyzing some key objectives and activities.

Performing a risk assessment requires defining and consistently applying an approach that is tailored to the organization. Any risk assessment exercise should begin with the establishment of a scope and plan, considering objectives, responsibilities, timing, and input and output requirements.

Below is an overview of the 6 steps that are covered in the Quick Scan

- Identify top 3 relevant business objectives

Objectives are defined at various levels of the organization (e.g., division, location, enterprise-wide), and it is important to understand how they are developed. SWOT analyses can help to define objectives.

	Level	Business objective
1.		
2.		
3.		

Risk analysis

- Identify events that could affect the objectives

Events that could affect the objectives can be categorized into two parts: external risks and internal risks. Using the check boxes below, select which types of risks that could affect your company's objectives.

Objective 1:			
External	Type of external risk	**Internal risk**	Type of internal risk
Economic	☐ Financial markets ☐ Unemployment ☐ Mergers & Acquisitions ☐ Competition	Infrastructure	☐ Availability of assets ☐ Capability of assets ☐ Access to capital ☐ Complexity
Natural environment	☐ Financial viability ☐ Quality of execution ☐ Service level agreements	Personnel	☐ Employee capability ☐ Fraudulent activity ☐ Health and safety
Political	☐ Laws and regulations ☐ Government / policy changes	Process	☐ Capacity ☐ Design ☐ Execution ☐ Suppliers & dependencies
		Technology	☐ Data integrity ☐ Data & systems availability ☐ Development & deployment ☐ Maintenance ☐ Pipeline new products

For each of the above categories, the risk types can be specified in more detail e.g. Government / policy changes can be specified to "non-compliance with new legislation."

- Identify events that could affect the objectives (continued)

Objective 2:			
External	Type of external risk	**Internal risk**	Type of internal risk
Economic	☐ Financial markets ☐ Unemployment ☐ Mergers & Acquisitions ☐ Competition	Infrastructure	☐ Availability of assets ☐ Capability of assets ☐ Access to capital ☐ Complexity
Natural environment	☐ Financial viability ☐ Quality of execution ☐ Service level agreements	Personnel	☐ Employee capability ☐ Fraudulent activity ☐ Health and safety
Political	☐ Laws and regulations ☐ Government / policy changes	Process	☐ Capacity ☐ Design ☐ Execution ☐ Suppliers & dependencies
		Technology	☐ Data integrity ☐ Data & systems availability ☐ Development & deployment ☐ Maintenance ☐ Pipeline new products

For each of the above categories, the risk types can be specified in more detail e.g. Government / policy changes can be specified to "non-compliance with new legislation."

- Identify events that could affect the objectives (continued)

Objective 3:			
External	Type of external risk	**Internal risk**	Type of internal risk
Economic	☐ Financial markets ☐ Unemployment ☐ Mergers & Acquisitions ☐ Competition	Infrastructure	☐ Availability of assets ☐ Capability of assets ☐ Access to capital ☐ Complexity
Natural environment	☐ Financial viability ☐ Quality of execution ☐ Service level agreements	Personnel	☐ Employee capability ☐ Fraudulent activity ☐ Health and safety
Political	☐ Laws and regulations ☐ Government / policy changes	Process	☐ Capacity ☐ Design ☐ Execution ☐ Suppliers & dependencies
		Technology	☐ Data integrity ☐ Data & systems availability ☐ Development & deployment ☐ Maintenance ☐ Pipeline new products

For each of the above categories, the risk types can be specified in more detail e.g. Government / policy changes can be specified to "non-compliance with new legislation."

- Determine risk tolerance and/or appetite

Risk tolerance is the acceptable level of variation. Risk tolerance considers the relative importance of risk types and aligns with risk appetite (e.g. high/medium/low). Risk tolerances should be defined for each key risk type identified above. Looking at the tolerances for multiple objectives allows management to better allocate resources to ensure reasonable likelihood of achieving outcomes across multiple objectives.

Objective	Risk types identified above	Accepted level of variation	Risk appetite
1.			
2.			
3.			

7

Risk analysis

- Assess likelihood and impact of risks

Events identified as potentially impeding the achievement of objectives are deemed to be risks and should be evaluated based on the likelihood of occurrence and the significance of their impact on the objectives. It is important to first evaluate such risks on an inherent basis. An impact and probability rating should then be assigned using defined risk rating scales. In the table below, fill out the various risk factors per object and highlight them with the appropriate label. For example, a risk factor identified above may be non-compliance with laws. However, this is a decreasing risk and the likelihood, as well as the impact of it, is relatively low.

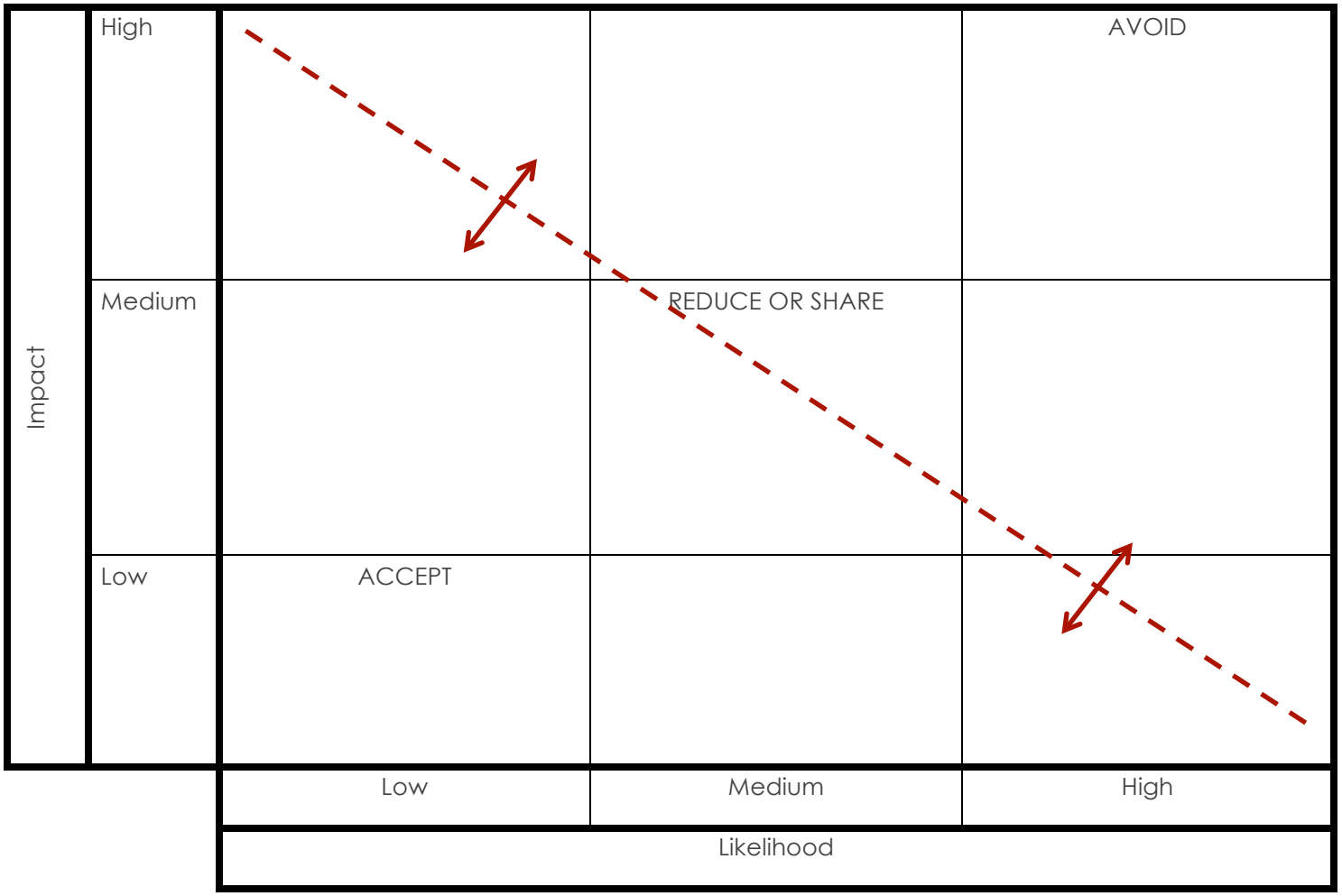
Impact				
	High			
	Medium			
	Low	E.g. Non-compliance with new legislation		
		Low	Medium	High
		Likelihood		

Increasing risk = Stable risk = Decreasing risk =

Risk analysis

- Evaluate risk and the response to each risk

For each of the risks identified and mapped above, a response strategy needs to be formulated. Typical risk response strategies are to accept, share, reduce, or avoid. The dotted line can be moved to fit what the response the company finds acceptable.



- Assess residual risk and likelihood of impact

Residual risk assessment considers both the risks as previously identified and the related risk response mechanisms and control activities in place to determine the impact and probability of their occurrence. In other words, it evaluates the adequacy and effectiveness of the internal checks and balances in place, providing reasonable assurance that the likelihood and impact of an adverse event is brought down to an acceptable level.