Risk Management Fact Sheet 1:
Risk Identification Techniques/Sources

Risk Management Process

Aim of the fact sheet

This fact sheet aims to help DETE staff members engaged in planning and risk management activities to understand:

- the importance of the risk identification step
- some methods and sources for identifying risks
- other considerations associated with identifying a risk.
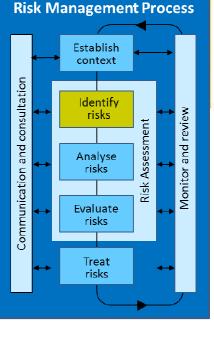
Why is risk identification important?

Identifying risks is the first and perhaps the most important step in the risk management process. It involves generating a comprehensive list of threats and opportunities based on events that might enhance, prevent, degrade, accelerate or delay the achievement of your objectives. If you don't identify a risk, you can't manage it.

It's also important to scan the environment from time to time to identify new and emerging risks, as the department's exposure to risk may be constantly changing.

How do I identify risks?

Identifying risks is a key step in a proactive risk management process. As part of this process you must look at the following sources:

Sources	Description
Risk registers and risk reports	Provide a foundation for evaluating existing risks and their potential risk to an objective.
Issues log	Record of issues faced and the actions taken to resolve them. Any issues that were formally identified as risks should be analysed.
Audit reports	Independent view of adherence to regulatory guidelines including a review of compliance preparations, security policies, access controls and management of risks.
Business Impact Analysis (BIA)	Detailed risk analysis that examines the nature and extent of disruptions and the likelihood of the resulting consequences.
Internal & external reviews	Reviews undertaken to evaluate the suitability, adequacy and effectiveness of the department's systems, and to look for improvement opportunities.

There is no easy scientific method that will guarantee you will identify all risks. Some additional better practice approaches to and sources for identifying risks include:

Approach /Sources	Description
SWOT analysis (Strength, Weakness, Opportunity Threats)	Commonly used as a planning tool for analysing a business, its resources and its environment by looking at internal strengths and weaknesses; and opportunities and threats in the external environment
PESTLE (Political, Economic, Sociological, Technological, Legal, Environmental)	Commonly used as a planning tool to identify and categorise threats in the external environment (political, economic, social, technological, legal, environmental)
Brainstorming	Creative technique to gather risks spontaneously by group members. Group members verbally identify risks in a 'no wrong answer' environment. This technique provides the opportunity for group members to build on each other's ideas
Scenario analysis	Uses possible (often extreme) future events to anticipate how threats and opportunities might develop.
Surveys/Questionnaires	Gather data on risks. Surveys rely on the questions asked.
One-on-one interviews	Discussions with stakeholders to identify/explore risk areas and detailed or sensitive information about the risk.
Stakeholder analysis	Process of identifying individuals or groups who have a vested interest in the objectives and ascertaining how to engage with them to better understand the objective and its associated uncertainties
Working groups	Useful to surface detailed information about the risks i.e. source, causes, consequences, stakeholder impacted, existing controls
Corporate knowledge	History of risks provide insight into future threats or opportunities through: • *Experiential knowledge* – collection of information that a person has obtained through their experience. • *Documented knowledge* – collection of information or data that has been documented about a particular subject. • *Lessons learned* – knowledge that has been organised into information that may be relevant to the different areas within the organisation.
Process analysis	An approach that helps improve the performance of business activities by analysing current processes and making decisions on new improvements.
Other jurisdictions	Issues experienced and risks identified by other jurisdictions should be identified and evaluated. If it can happen to them, it can happen here.

What information should we collect during the risk identification step?

Identifying risks involves considering what, when, why, where and how things can happen. More specifically:

- **What are the sources of risk or threat** – the things which have the inherent potential to harm or facilitate harm.

- **What could happen** – events or incidents that could occur whereby the source of risk or threat has an impact on the achievement of objectives.
- **Where** – the physical locations/assets where the event could occur or where the direct or indirect consequences may be experienced.
- **When** – specific times or time periods when the event is likely to occur and/or the consequences realised.
- **How** – the manner or method in which the risk event or incident could occur.
- **Causes** – what are the direct and indirect factors that create the source of risk or threat.
- **Business consequences** – what would be the impact on objectives if the risk was realised.
- **Business areas/stakeholders affected** – what parts of the organisation and what stakeholders might be involved or impacted?
- **Existing controls** – a preliminary review of existing controls should be undertaken to identify
  - **What controls currently exist** to minimise the likelihood and consequences of each risk?
  - **What vulnerabilities exist** that could undermine the effectiveness of the controls?

Note: a detailed review is completed during the risk analysis process.

Other considerations

Risks relating to multiple objectives

A risk may be related to more than one of the department's objectives and/or its potential impact may vary in relation to different objectives, and the best way of addressing the risk may be different in relation to different objectives. Risk identification may therefore require different levels of analysis.

Risk statements

It is important to express the identified risks as specifically as possible in relation to the objective. Otherwise the ability to assess and manage the risk will be less than effective.

In stating risks, avoid:
- stating impacts which may arise as being the risks themselves
- including risks which do not impact on objectives
- including risks which are simply the converse of the objectives.

To avoid poor expressions of the risk, the risk statement should encompass the uncertain event (or uncertainty), the cause or event that trigger the risk and its consequence/impact.

ERM Fact Sheet 3: Risk statement provides more guidance on writing a good quality risk statement.

Risk ownership

Once risks are identified, they should be assigned a risk owner who has responsibility for ensuring that the risk is being managed and monitored.

Risk categories

Risks during this initial phase of the process should also be allocated a risk category.

ERM Fact Sheet 4 Risk categories provides more guidance on allocating a risk to a risk category