Is it time to rethink risk management?

by Abeeda Ladha

good-governance.org.uk

BLOG

GGI consultant Abeeda Ladha encourages us all to think a little differently about risk.

For most people, the first thought that comes to mind when risk is mentioned will be a negative one.

The Oxford English Dictionary defines risk as a noun, meaning a situation involving exposure to danger, and as a verb, meaning to expose someone or something valued to danger, harm, or loss.

Until now, the NHS has based its risk management on the Australian Standards AS/NZS 4360:2004, but with the publication of the ISO 31000:2009 standards, is there an opportunity to change how risk is perceived?

The ISO 31000:2018 difference

ISO 31000:2018 provides guidelines on managing the risks organisations face in any industry or sector and is applicable to any type of risk, regardless of its nature or consequence.

In the AS/NZS 4360:2004 standard, risk is defined as the 'chance of something happening that will impact on objectives', while ISO 31000:2018 defines risk as the 'effect of uncertainty on objectives' where an effect is a positive or negative deviation from what is expected.

The new definition moves away from the possibility of an event happening and instead emphasises the effect on objectives.

Uncertainty is the lack of information / knowledge concerning an event, its consequence or likelihood positive or negative

Effect → of → Uncertainty → on → Objectives

An effect is a deviation from what was expected, which can be either positive or negative

Activity undertaken to reach goals.

What is the point of risk management?

ISO 31000 describes the purpose of risk management as to create and protect value, improve performance, encourage innovation and support the achievement of objectives.

To achieve effective risk management, the eight principles defined by the standard are:

1. Integrated – risk management is an integral part of all organisational activities.
2. Structured and comprehensive – a structured and comprehensive approach contributes to consistent and comparable results.
3. Customised – the risk management framework and processes are customised and proportionate to the organisation's external and internal context related to its objectives.
4. Inclusive – appropriate and timely involvement of stakeholders results in improved awareness and informed risk management.
5. Dynamic – risk management anticipates, detects, acknowledges and responds to changes and events in an appropriate and timely manner.
6. Informed – information should be timely, clear and available to relevant stakeholders.
7. Audience-appropriate – the design of the risk framework and communication about risk should take into account the cultural characteristics and level of knowledge of the audience.
8. Always improving – risk management is continually improved through learning and experience.

These principles should enable an organisation to manage the effects of uncertainty on its objectives.

Achieving the principles

To support and sustain risk management within an organisation, ISO 31000 outlines six elements:

- *Leadership and communication* – commitment from leaders at all levels of the organisation
- *Integration* – risk management integrated into all aspects of the organisation and decision making
- *Design* – planning risk management – allocating resources, establishing communication channels, etc
- *Implementation* – implementing risk management plans into practise
- *Evaluation* – reviewing and analysing the processes in place, measuring success
- *Improvement* – monitoring the framework, addressing internal and external changes and continuously making improvements where needed.

Viewed through a slightly different lens, the last four of these elements constitute a Plan-Do-Study-Act (PDSA) process supporting the continuous improvement of risk management processes.

The risk management process

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

ISO 31000 states that leadership should ensure that risks are prioritised according to how they can create and deliver value rather than the current approach of ranking risks by their likelihood and impact.

What is positive risk?

A positive risk would be one that has a positive impact on the objectives of an organisation. As their impact is positive, they can be referred to as opportunities. Positive risks can materialise from changes in policy, or technology that is currently under development that will save resources if released.

Although the idea may seem counterintuitive, positive risks can be good for organisations. Examples include a risk taken in a supply chain resulting in early delivery, or the adoption of new technology resulting in a fall in the time it takes to complete a task, or perhaps a project delivered under the assigned budget which can then be utilised elsewhere.

Instead of the traditional doom and gloom on risk registers, is it time that the NHS embraced adding positive risks to its board assurance frameworks and strategic risk registers, to achieve a balanced overview of the 'effect of uncertainty' on the objectives of the organisations?

We have heard CEOs and CFOs talking about positive risks – is it time for a revamp of the way the NHS practises risk management? GGI certainly thinks so.

We think a shift to practising risk management with both positive and negative risks would help to create a proactive and continuous improvement culture – which is what risk management is supposed to be all about – and thereby create and protect value for organisations.

GGI already supports organisations with their risk management through workshops and training and this can easily be enhanced to introduce ISO 31000 risk management standards for any organisations looking to adopt these.

GGI is already looking to review its own internal risk management guidelines to reflect the ISO 31000 and can support organisations to do the same. Please don't hesitate to contact us if you feel we might be able to help you.