



# NEBOSH IIRSM Certificate in Managing Risk



# Contents

|                                                                                                                    |            |
|--------------------------------------------------------------------------------------------------------------------|------------|
| <b>Introduction</b>                                                                                                | <b>04</b>  |
| <b>Element 1 Principles of risk and risk management</b>                                                            | <b>06</b>  |
| 1.1 The principles of risk and risk management                                                                     | 07         |
| 1.2 The impact of psychology on decision-making                                                                    | 26         |
| <br>                                                                                                               |            |
| <b>Element 2 The risk management process</b>                                                                       | <b>44</b>  |
| 2.1 Overview of the risk management process                                                                        | 45         |
| 2.2 Scope, context and risk appetite                                                                               | 49         |
| 2.3 Risk assessment                                                                                                | 75         |
| 2.4 Risk treatment                                                                                                 | 90         |
| 2.5 The role and importance of risk reporting and information                                                      | 94         |
| 2.6 Communication and consultation in the risk management process                                                  | 98         |
| 2.7 Monitoring and review of the risk management process                                                           | 102        |
| <br>                                                                                                               |            |
| <b>Element 3 The risk management framework</b>                                                                     | <b>104</b> |
| 3.1 Integrating the risk management framework within an organisation                                               | 105        |
| 3.2 The risk management framework and its relationship with culture                                                | 122        |
| 3.3 The relationship between risk management, business continuity, crisis management and organisational resilience | 128        |

Edition: 1  
Version: 1

Contains public sector information licensed under the Open Government Licence v1.0.

Every effort has been made to trace copyright material and obtain permission to reproduce it. If there are any errors or omissions, NEBOSH would welcome notification so that corrections may be incorporated in future reprints or editions of this course book.

© NEBOSH 2020  
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form, or by any means, electronic, electrostatic, mechanical photocopied or otherwise, without the express permission in writing from NEBOSH.

## Introduction

We are living in very complicated and disrupted times. It has never been so important for individuals and organisations to reduce threats and maximise opportunities. Think climate change, cyber threats, complex regulatory environments, data breaches, Covid-19 pandemic and levels of anxiety in the workforce. The wildfires in Australia and California and the floods in the UK are just some examples of the pressures on organisations to act on climate risk, while managing many other risks, and still being expected to meet shareholder, financial, regulatory, customer and ethical expectations.

According to Mark Zuckerberg, "The biggest risk is not taking any risk. In a world that's changing quickly, the only strategy that is guaranteed to fail is not taking risks". We can apply this statement to all of us because we are all 'managers of risk'. Whatever our role, we make decisions that involve an element of risk, but the critical point is do we know how to effectively identify, evaluate and manage these risks?

In today's environment, working together across all stakeholders is the only way to truly manage significant risks, whether at an organisation, operational or project level. Everyone is responsible. The only way to protect people, reputation and profits is by embedding risk management into decision-making together with creating a culture that encourages honesty and openness, direct feedback and a willingness to admit mistakes and ask for help.

Although many organisations talk about being compliant and better able to report on risk, the reality is that many still don't invest in improving their risk capabilities. Think Carillion, Oxfam, Alton Towers, British Airways, Grenfell, Kodak, Toys R Us, Enron, Wells Fargo, Siemens, Volkswagen and #metoo.

The NEBOSH IIRSM Certificate in Managing Risk is the perfect qualification for those who need to be equipped to identify, evaluate and manage risks and to understand their impact for the organisation.

By studying this qualification, you will gain transferrable skills that can be used in any organisation, industry and job. You will learn:

- the principles of risk and risk management
- the risk management process and framework based on ISO 31000
- the relationship between psychology and decision-making
- how to analyse the environment in which an organisation operates, identifying potential risks and opportunities
- the relationship between risk management, business continuity, crisis management and organisational resilience.

NEBOSH and IIRSM would like to thank the many contributors that have helped develop this qualification, and we really hope you enjoy studying it and find it rewarding. Good luck!

### Qualification structure

This study guide supports the NEBOSH IIRSM Certificate in Managing Risk Effectively. It is divided into three elements. These are:

- Element 1 - Principles of risk and risk management
- Element 2 - The risk management process
- Element 3 - The risk management framework

# "The biggest risk is not taking any risk..."

## "In a world that's changing really quickly, the only strategy that is guaranteed to fail is not taking risks".

Mark Zuckerberg (October 2011)

Mark Zuckerberg is a university drop out, technology entrepreneur, philanthropist, and billionaire. He is most well-known for creating the Facebook application.



# Element 1

## Principles of risk and risk management

This element sets out a basis of risk and explores why some people are more willing to take risks than others. It is split into two parts.

- 1.1 The principles of risk and risk management
- 1.2 The impact of psychology on decision-making

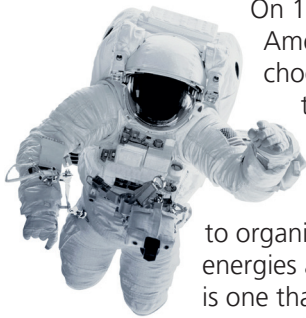
At the end of this element you will be able to:

- Recognise different definitions of risk
- Understand the common themes across different risk definitions
- Recognise positive consequences of risk
- Distinguish between uncertainty, risk, and hazard
- Identify uncertainty using credible sources of information
- Recognise the value of information
- Identify and classify types of risk
- Understand the principles of risk management
- Describe experimental and personality-based approaches to risk psychology
- Appreciate why people think and act differently
- Describe the benefits of diverse thoughts on risk
- Demonstrate how human thought influences decision making
- Understand how behavioural economics can influence decision making.

## 1.1 The principles of risk and risk management

### Different definitions of Risk

Risk means different things to different people. In this section we will explore how our perception of risk is defined by our awareness of our circumstances.



On 12 September 1962 John F. Kennedy, American President, famously said "We choose to go to the moon. We choose to go to the moon in this decade and do the other things, not because they are easy, but because they are hard, because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one which we intend to win, and the others, too".

#### Did you know...

In 1950s and 1960s America, the lunar landings were made possible by the work of Black African American women mathematicians, engineers and scientists like Katherine Johnson, Mary Jackson, and Dorothy Vaughan. You can read more about this on the NASA web site.

Obviously, there were many risks to be managed but alongside this were great opportunities which made the mission worthwhile.

On 20 July 1969 the world watched as a 10 metre wide lunar module successfully landed on the surface of the moon, 385,000km away.

Today, extreme weather events mean staying at home can be just as hazardous.

Wildfires in America and Australia, flooding in Europe and Asia, and water shortages in Africa have all caused loss of life.

#### Did you know...

The Australasian Fire Authorities Council adopt ISO31000 as the standard of risk management for all firefighting and mitigation operations. Greg Penney has published interesting research on this. ([www.mdpi.com/2571-6255/2/2/21](http://www.mdpi.com/2571-6255/2/2/21))

In November 2018, at least 88 civilians were killed by fires in California. The fire destroyed more than 10,000 structures.

According to the UK Government, more than 5 million people live and work in 2.4 million properties that are at risk of flooding from rivers or the sea, one million of which are also at risk of surface water flooding. A further 2.8 million properties are susceptible to surface water flooding alone.

### Activity

What does risk mean to you?



No matter who you are, where you are, and what you do, risk means something that is unique to you. Here are some examples of risk definitions from a range of disciplines:

"The likelihood of potential harm from a hazard being realised" – British Health and Safety Executive (HSE).

"Actual or potential threat of adverse effects on living organisms and environment by effluents, emissions, wastes, resource depletion, etc., arising out of an organization's activities" – Environmental Science.

"Significant conditions, events, circumstances, actions, or inactions that could adversely affect an entity's ability to achieve its objectives and execute its strategies, or from the setting of inappropriate objectives and strategies." – International Accounting Standards (IAS315).

"A Risk is an uncertain event or condition that if it occurs, has a positive or negative effect on a Project's Objectives" Project Management Book of Knowledge or "An uncertain event that if it occurs, will have a positive or negative effect on project objectives" – PRINCE2.

Operational risk has been described in the banking industry as "the risk of loss, resulting from inadequate or failed internal processes, people and systems, or from external events" – Basel Committee on Banking Supervision.

"Risk happens because we have a purpose, we make decisions and the outcomes are uncertain" – Grant Purdy, widely recognised Risk Management Professional.

"Risk arises from the interactions between objectives (what must happen) and uncertainty (what might happen). Therefore, risk is uncertainty that matters." – Academic definition produced by Dr David Hillson.

Risk is "the combination of impact (the potential harm that could be caused) and probability (the likelihood of the particular issue or event occurring)" – Financial Conduct Authority definition (FCA).

Risk is the "effect of uncertainty on objectives" – International Organization for Standardizations (ISO) risk management standard ISO 31000:2018.

**Different organisations often have their own definitions of risk**

For example, a financial institution would consider risk quite differently to a manufacturer or charity. It would not be unusual for different types of organisations in the same sector to have different attitudes to risk – consider the differences between a small independent clothing shop and a global clothing company. The UK's Oxford University Hospitals NHS Foundation Trust define risk as "Achievement of objectives is subject to uncertainty, which gives rise to threats and opportunities". Uncertainty of outcome is how risk is defined. Risk management includes identifying and assessing risks and responding to them.

It is important that you understand what risk means to your organisation.

Activity

What does risk mean to your organisation?

Clue: You might find this information in the risk policy or in the annual accounts.

**An international standard definition of 'Risk'**

In February 2018, the International Organization for Standardization (ISO) approved the new risk management standard ISO 31000:2018. We have already looked at a variety of risk definitions; although this study guide will explore risks across a variety of industries and functions, for consistency, the ISO 31000 definition of risk will be used (as this is internationally recognised):

The "effect of uncertainty on objectives".

ISO 31000 describes 'effect' as a deviation from the expected. It can be positive, negative, or both, and can create or result in opportunities and threats. It does not define objectives, but it does recognise that objectives can:

- have different aspects and categories, and
- be applied at different levels.



Activity

What are your organisation's strategic objectives?

Clue: You might find your organisation's objectives in its annual report.



## Common themes across risk definitions

Although there are lots of definitions of risk, they tend to share common elements. These are described below.

A **risk source** is an element which alone or in combination with others has the potential to give rise to a risk. A risk source may sometimes be referred to as a cause.

Risk causes are sometimes broken down into immediate causes, underlying causes (the circumstances that created the immediate cause), and root causes (the organisational factors that created the circumstances in which the cause could exist).

### A risk has a source.

An **event** can be either an occurrence or a change of a particular set of circumstances. Although the term 'event' is used, it could have more than one occurrence, more than one source, and more than one consequence.

It could be something unexpected, or it could be something expected which does not happen.

### An event is a consequence of a risk occurring.

**Level of risk** is the magnitude or scale of a risk or combination of risks, expressed in terms of the combination of consequences and likelihood.

**Likelihood** is the chance of something happening.

**Consequence** is the outcome of an **event** on objectives. In the same way that sources can be broken down into immediate, underlying and root causes, so consequences can be broken down into immediate, subsequent, and ultimate effects. An incident at work (immediate) could lead to a late delivery or cancelled order, which in turn could result in a lost customer, or financial difficulties.

### NASA Space Shuttle Challenger Explosion

Decisions to build components off site was one of the factors that led to the explosion of the Space Shuttle Challenger with the loss of all seven lives on board – including a civilian schoolteacher.

The event could have been avoided; technical design failings were known. On the day of the take-off, it was particularly cold. It was known that cold weather could (and probably would) exacerbate the technical problem.

Factors such as the educational value of the trip (17 million Americans watched the launch) and the US President planning to talk about the space mission at the annual 'state of the nation' speech that evening influenced the go/no-go decision to launch. A decision that would ultimately backfire catastrophically.

A **control** is a measure that maintains and/or modifies the risk.

For this reason, a 'control' can include processes, policies, devices, practices, or other circumstances or interventions.

### Risks can have many controls.



**Significant risks** are those which can have an impact on objectives.



For example, a raw chicken delivery to a restaurant that is 10 minutes late might not be significant, but a collapse in the supply chain that results in 900 fast food outlets closing temporarily and the police force in London, UK tweeting "please do not contact us #KFCCrisis" is significant. KFC had changed their UK haulage contractor. ([www.bbc.co.uk/news/uk-england-coventry-warwickshire-43142498](http://www.bbc.co.uk/news/uk-england-coventry-warwickshire-43142498))

A **Stakeholder** is defined as a person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity (this could include customers and suppliers, shareholders, and employees, but could also include environmental protestors such as those campaigning against the practise of fracking).

### A risk can affect the objectives of the organisation or its stakeholders.

**Uncertainty** is a feature of many risk definitions. Some authors suggest that once you know that a risk is going to happen, it ceases to be a risk.

Uncertainty arises when something cannot be relied upon or when something is not known or not definite.

### Emerging Risks are:

- a. current risks evolving in unexpected ways or with unforeseen consequences, or
- b. new risks that have never been seen before.

When we think back in history, we can see some spectacular examples of the unexpected coming true, often by highly respected and well-known leaders in their respective fields:

- "Heavier-than-air flying machines are impossible. X-rays will prove to be a hoax." William Thomson, Lord Kelvin, British scientist, 1899.
- "There is not the slightest indication nuclear energy will ever be obtainable." Albert Einstein, 1932.
- "I think there is a world market for maybe 5 computers" Thomas Watson, IBM President, 1943.
- "There is no reason anyone would want a computer in their home." Ken Olsen, DEC Founder, 1977.

It is not easy to see risks (opportunities or threats) that we are not used to seeing.

Few people would have predicted the development of the mobile phone, let alone the smart phone that many of us use today, or the production of a tablet computer without a keyboard or mouse.

### Did you know...

In February 2002, Donald Rumsfeld, US Secretary of State for Defence, was widely ridiculed for saying "There are known knowns. There are things we know that we know. There are known unknowns. That is to say, there are things that we now know we don't know. But there are also unknown unknowns. There are things we do not know we don't know." Since then, it has been widely used in a range of technical and scientific literature.



This book is suitable for anyone who needs to be able to identify, evaluate and manage risks and to understand their impact on an organisation. It covers:

- principles of risk and risk management;
- the validity of risk information;
- the impact of psychology on decision making;
- how to apply the risk management process to manage risk effectively (based on ISO 31000); and
- how to integrate the risk management framework into an organisation.

The content follows the syllabus for the NEBOSH IIRSM Certificate in Managing Risk qualification and can be used as part of your studies. Even if you are not studying this qualification, this book is an invaluable reference source and practical guide for those requiring an understanding of risk management.





**RMBK0221**

ISBN: 978-1-913444-09-9



9 781913 444099 >

#### Follow us:

-  [www.linkedin.com/company/nebosh](https://www.linkedin.com/company/nebosh)
-  [www.facebook.com/neboshofficial](https://www.facebook.com/neboshofficial)
-  [@NEBOSHTweets](https://twitter.com/NEBOSHTweets)
-  [www.youtube.com/neboshofficial](https://www.youtube.com/neboshofficial)

#### NEBOSH

5 Dominus Way  
Meridian Business Park  
Leicester LE19 1QW  
United Kingdom

[info@nebosh.org.uk](mailto:info@nebosh.org.uk)  
[www.nebosh.org.uk](https://www.nebosh.org.uk)

NEBOSH, the National Examination Board in Occupational Safety and Health,  
is a world leading provider of health, safety, environmental and wellbeing qualifications.

Registered in England and Wales | Company number: 2698100 | Registered charity number: 1010444

© Copyright NEBOSH 2020