

# Integrated safety, health and environmental management



This item contains selected online content. It is for use alongside, not as a replacement for the module website, which is the primary study format and contains activities and resources that cannot be replicated in the printed versions.

## About this free course

This free course provides a sample of level 3 study in Computing & IT

<http://www.open.ac.uk/courses/find/computing-and-it>

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University:

<http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/integrated-safety-health-and-environmental-management-introduction/content-section-0>.

There you'll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

The Open University, Walton Hall, Milton Keynes, MK7 6AA, United Kingdom

Copyright © 2016 The Open University

## Intellectual property

Unless otherwise stated, this resource is released under the terms of the Creative Commons Licence v4.0 [http://creativecommons.org/licenses/by-nc-sa/4.0/deed.en\\_GB](http://creativecommons.org/licenses/by-nc-sa/4.0/deed.en_GB). Within that The Open University interprets this licence in the following way:

[www.open.edu/openlearn/about-openlearn/frequently-asked-questions-on-openlearn](http://www.open.edu/openlearn/about-openlearn/frequently-asked-questions-on-openlearn). Copyright and rights falling outside the terms of the Creative Commons Licence are retained or controlled by The Open University. Please read the full text before using any of the content.

We believe the primary barrier to accessing high-quality educational experiences is cost, which is why we aim to publish as much free content as possible under an open licence. If it proves difficult to release content under our preferred Creative Commons licence (e.g. because we can't afford or gain the clearances or find suitable alternatives), we will still release the materials for free under a personal end-user licence.

This is because the learning experience will always be the same high quality offering and that should always be seen as positive – even if at times the licensing is different to Creative Commons.

When using the content you must attribute us (The Open University) (the OU) and any identified author in accordance with the terms of the Creative Commons Licence.

The Acknowledgements section is used to list, amongst other things, third party (Proprietary), licensed content which is not subject to Creative Commons licensing. Proprietary content must be used (retained) intact and in context to the content at all times.

The Acknowledgements section is also used to bring to your attention any other Special Restrictions which may apply to the content. For example there may be times when the Creative Commons Non-Commercial Sharealike licence does not apply to any of the content even if owned by us (The Open University). In these instances, unless stated otherwise, the content may be used for personal and non-commercial use.

We have also identified as Proprietary other material included in the content which is not subject to Creative Commons Licence. These are OU logos, trading names and may extend to certain photographic and video images and sound recordings and any other material as may be brought to your attention.

Unauthorised use of any of the content may constitute a breach of the terms and conditions and/or intellectual property laws.

We reserve the right to alter, amend or bring to an end any terms and conditions provided here without notice.

All rights falling outside the terms of the Creative Commons licence are retained or controlled by The Open University.

Head of Intellectual Property, The Open University  
The Open University

# Contents

Introduction	4
Learning Outcomes	5
1 Safety, health and environmental management – a risky business!	6
2 Setting priorities	10
3 Analysing incidents	13
3.1 Types of incident	13
3.2 Multiple causes	16
4 Integrated management	18
4.1 Introduction	18
4.2 Why integrate management systems?	25
5 Emergency planning	29
5.1 Introduction	29
5.2 Why plan?	30
5.3 Emergency planning as a formal requirement	30
5.4 Emergency planning as a public protection activity	31
5.5 Emergency planning as an organisational management function	32
5.6 Business continuity planning	39
5.7 Emergency planning – the process	41
Conclusion	47
Keep on learning	49
References	49
Acknowledgements	50

# Introduction

---

Life is full of risk. We encounter many uncalculated outcomes, some beneficial and others adverse. Businesses, especially in the financial context, often consider risk in terms of opportunities for gain. Risk in our context is a way of describing the probability and consequences of harm, or at worst a disaster. Risk management involves many stakeholders who can themselves influence the risks facing an organisation. Integrated management systems help ensure that safety, quality, environmental and business risks are managed right across an organisation. An integral part of management systems is emergency preparedness – the management of emergencies and disasters.

This OpenLearn course provides a sample of level 3 study in [Computing & IT](#)

# Learning Outcomes

---

After studying this course, you should be able to:

- define risk in the most appropriate way, and appreciate the need to prioritise risks
- appreciate the costs of illness associated with workplace activities
- describe in outline the development of models used to explain the cause of incidents and to promote prevention
- recognise the multiple causes contributing to many incidents, and be able to represent them diagrammatically
- illustrate the components of an integrated management system.

# 1 Safety, health and environmental management – a risky business!

While views on management differ, Safety, Health and Environmental (SHE) management is merely a subset of management to which the same generalities apply. Indeed, at the end of this free course we will see indications of the integrating concepts being promoted by organisations. However, for the present we can translate the key actions of management into:

**Plan** – anticipate problems before they occur, and plan for prevention rather than remedying problems. A hierarchical approach is fundamental in both health and safety as well as environmental protection, and the root cause of problems should be addressed at source.

**Organise** – work through the co-ordinated actions of everyone.

**Integrate** – SHE management is a multidisciplinary area embracing scientific, engineering, social and political issues. No individual can be expert in all of these disciplines, but the SHE manager should be able to appreciate the different perspectives and to recognise the trade-offs that are inevitable.

**Measure** – ‘When you can measure what you are speaking about and express it in numbers, you know something about it.’ So said Lord Kelvin, the scientist after whom the Kelvin scale of temperature is named. This is a particularly important approach in SHE management in which value judgements and opinions play a role that is the equal of facts. Only by deriving measures can we understand the issues better and seek to balance one against the other. However, we must understand the data and interpret them correctly.

**Control** – When problems have been identified and possible solutions proposed, the next step is to adopt implementation and control strategies to achieve the desired outcomes. The SHE manager must be able to understand the options and identify the most appropriate ones.

Implicit in these aspects of management is the process of evaluating alternative actions and selecting the most appropriate. This element is often called *risk management* and is the decision-making process involving consideration of political, social, economic and engineering information with risk-related information.

## So what is risk?

It is a word of such common usage that we all know its meaning.

### Activity 1

Before continuing, write down your definition of risk. Risk is ...

By writing your definition now you will be able to refer back to see whether your perception changes as you progress through this unit. We will meet the concept of risk in various sections and it will be dealt with from different perspectives by different authors. However, for the present, we can consider the following definitions.

First, the *Shorter Oxford English Dictionary* has the following definitions:

Risk

1. Hazard, danger, exposure to mischance or peril.
2. The chance or hazard of commercial loss, specifically in the case of insured property or goods.

### Activity 2

1. Compare your definition with the above definitions. Do they correspond?
2. Risk is equated with hazard in this definition. Do you agree with this?

Let us now look at three other definitions of risk given by The Engineering Council (1993, p. 2):

Risk is the chance of an adverse event.

Risk is the likelihood of a hazard being realised.

Risk is the combination of the probability, or frequency of occurrence, of a defined hazard and the magnitude of the consequences of the occurrence.\* It is therefore a measure of the likelihood of a specific undesired event and the unwanted consequences or loss.

\* *Definition in accordance with BS 4778: Section 3.1:1991 Quality Vocabulary*

### SAQ 1

How do these definitions match those from the *Oxford English Dictionary*?

#### Answer

You should notice the distinction in The Engineering Council definition between hazard and risk. The more detailed definitions associate risk with chance of an event occurring in much the same way as the OED definition refers to chance of financial loss. Hazard and risk are not the same and this will be developed later. Hazard is an intrinsic property of something with the capability of causing harm, whereas risk refers to the chances of that harm occurring. Did your definitions draw out these distinctions?

It is also important to note the meaning of risk in law. The legal case *R. v. Board of Trustees of the Science Museum* (Court of Appeal, Criminal Division, Times Law Report, 9 March 1993) was an appeal against a conviction in 1990 under Section 3(1) of the Health and Safety at Work, etc. Act 1974. The prosecution case was that the defendants had failed to maintain their air conditioning system to a sufficient standard and thereby had exposed the public to health risks from legionnaire's disease.

Section 3(1) of the Act places a duty on an employer to:

ensure, so far as is reasonably practicable, that persons not in his employment who may be affected thereby are not thereby exposed to risks to their health and safety.

The issue of legal concern was the interpretation of the phrase 'exposed to risks'. The prosecution case maintained that it was not necessary to prove that members of the

public had inhaled the *Legionella* bacterium, or even that it was present in the air. It was sufficient that there was a risk of it being there.

The Court of Appeal agreed with this interpretation, which implied ‘a possibility of danger’. Given the preventive nature of modern legislation, any view to the contrary would undermine enforcement.

‘Risk’ is not a term in major environmental legislation (specifically the Environmental Protection Act 1990 and water legislation), but the above ruling is consistent with that in the case of *National Rivers Authority v. Egger UK Ltd* from 1992. In that case the Court held that ‘polluting’ matter in water legislation implies a discharge capable of causing harm, but it is not necessary to prove that harm actually occurred. Similarly, in *HM Inspectorate of Pollution v. Drum Laundry Services* (June 1994), concerning a breach in the integrity of a bund surrounding a drum storage area, HMIP did not have to prove that environmental damage had occurred. It was sufficient that there had been a contravention of the authorisation conditions with the potential to cause harm.

So, any hazard may present a range of risk scenarios:

- risk to the health and safety of people at any level from stress, through physical injury to death;
- a risk of harm to the environment, including effects on plants, animals, materials and the environment itself in terms of climate etc. (e.g. global warming);
- a risk to the activity itself in terms of damage to equipment, delays or loss of production.

All three scenarios have a common element of financial loss associated with them, such as through compensation claims, fines after prosecutions under legal regulations, or economic losses from failing to meet contractual obligations to customers.

You may come across the ‘system boundary’ concept. It comes up, for example, in the context of issues such as energy analysis and life-cycle assessment. If you are familiar with these concepts you will recognise the importance of defining how far one should extend the boundary of study. Figure 1 represents the range of risk scenarios within system boundaries. You will see spatial dimensions of the system boundaries implicit in Figure 1 in practical contexts when we review several incidents later.

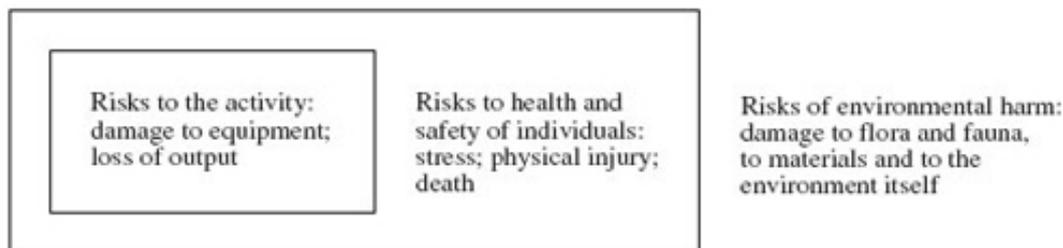


Figure 1 Risks to various systems

A different approach considers system boundaries in three dimensions. While the traditional health and safety focus is on workplace and similar local issues, introducing the environmental element widens the focus considerably such that the spatial dimension extends to the global scale. The other dimensions probably change very little. For example, there has long been concern about the long-term health issues of workplace as well as environmental contaminants. On the three-dimensional system in Figure 2 we have illustrated several events ranging from the international and long-term impact of the

incident at the nuclear power station at Chernobyl, with its implications for many people, through the medium-term impact of an earthquake such as that in Japan in 1995, to the relatively short-term effect of annoyance to an individual by loud noise.

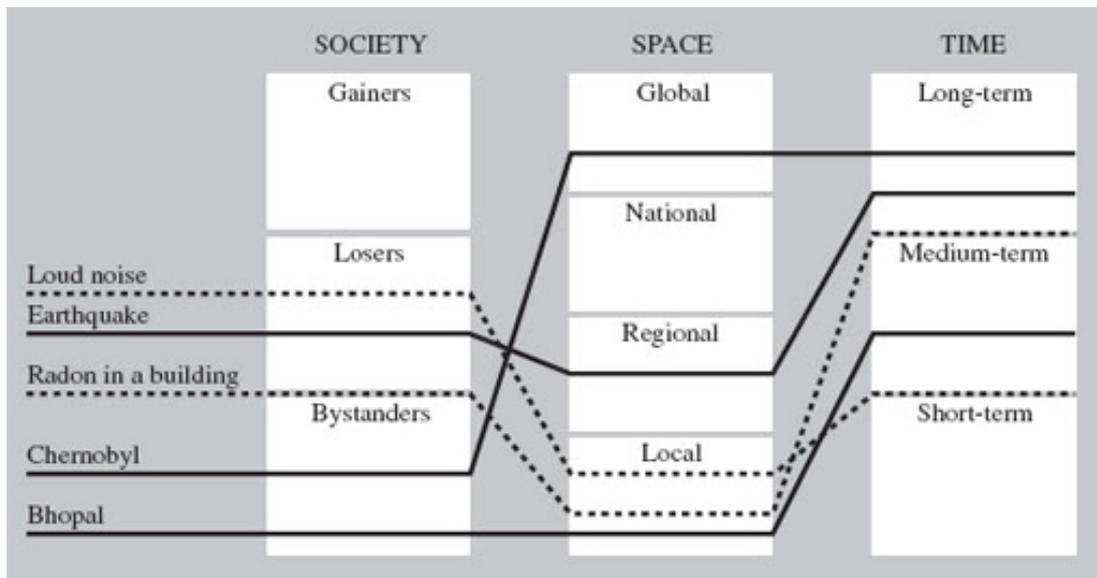


Figure 2 Dimensions of safety, health and environmental concerns

There are also uncertainties associated with any placing within the boxes in Figure 2. For example, asbestos has long been used to great advantage in fire protection, so many people have gained from its use. However, as its health implications became more and more apparent, the numbers of losers increased and certainly the time scales increased. In October 1995 a High Court ruled for the first time that compensation was payable to those suffering harm by living or playing as children close to an asbestos plant. Previous cases covered only those working at the plant. The judge ruled that from 1933 onwards, when the claimants were living in the area, the defendants must have known of the dangers to them of the asbestos dust, and had taken no reasonable steps to reduce or prevent the emissions. The liability related specifically to mesothelioma, a form of cancer of which the only known cause is asbestos. You might also like to consider other incidents, such as aircraft or ferry disasters, and where they should be placed on Figure 2. Your views may differ from ours, but the main point is to make you think about the implications of such incidents over the various dimensions.

The perspective represented in Figure 2 suggests that a wide variety of issues and examples could be included in this unit. Unfortunately, constraints on your study time and the size of this unit dictate that we can deal with only a limited range of issues. However, the intention is that many of the skills and much of the knowledge will be transferable to dealing with other SHE problems and issues.

## 2 Setting priorities

### Activity 3

Consider whether the relative economic aspects should determine the degree of priority given to different aspects of the risk scenarios in [Figure 1](#).

It should be clear from Figures [1](#) and [2](#) that the range of incidents a manager could examine, and similarly the range that we could consider in this unit, extends from disasters to relatively minor inconveniences. While the local event is of concern to most individuals, major incidents receive greatest publicity and raise more general concerns about the risks of technology. In fact, the perceptions of risk are not based solely on quantitative measures but include subjective value judgements. These may be influenced by the degree to which the risk is imposed upon us rather than accepted voluntarily, our knowledge of the problem, our trust in the 'management' of the risk and so on, but more of that later. The net result is that reaching a consensus view can be difficult. Later in this unit we will explore some specific incidents in greater detail. For the present, however, we can accept that such major industrial incidents have important consequences in terms of death, ill health, and environmental and economic impact.

Returning to our question about setting priorities, the economic factor may not be a reliable one for setting priorities because it is difficult to place economic value on the cost of human life and illness and on the costs of environmental harm. Certainly the area of environmental economics is a developing one but it will not be considered further here.

The first detailed study of the cost of accidents was made in 1931 by Heinrich (see Heinrich, 1990). By examining many thousands of insurance records and interviewing many staff he derived a statistical relationship that the uninsured costs (he called these the indirect costs) were typically four times higher than the direct costs covered by insurance. This relationship is commonly represented as an iceberg (Figure 3).

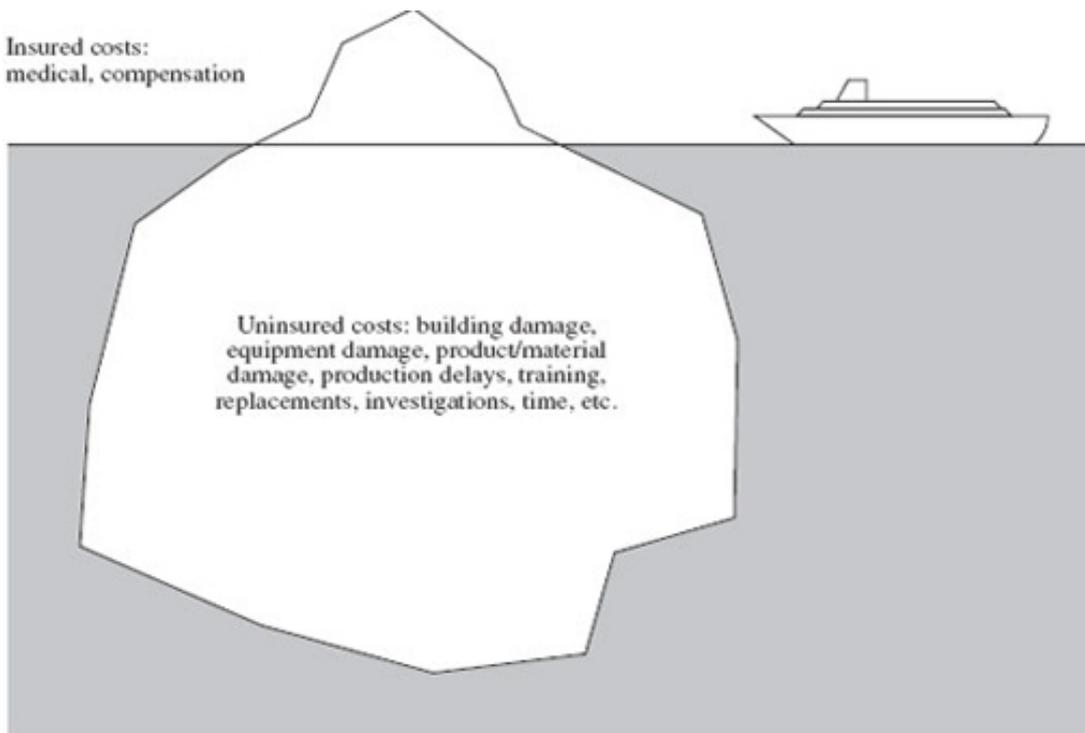


Figure 3 Insured costs are the tip of the iceberg

In the UK, companies are required by law to have employers' liability insurance cover, but cover for the other aspects of potential loss depends on many factors, including the availability and cost of cover as well as the organisation's perception of the risks of such loss. Heinrich also developed the concept of a non-injury accident. He defined this as an unintended event that causes property loss by damage to plant, equipment or materials, but does not cause actual injury, although it may have the potential to do so. Such events are many times more common than those involving injury, as his accident triangle illustrates (Figure 4).

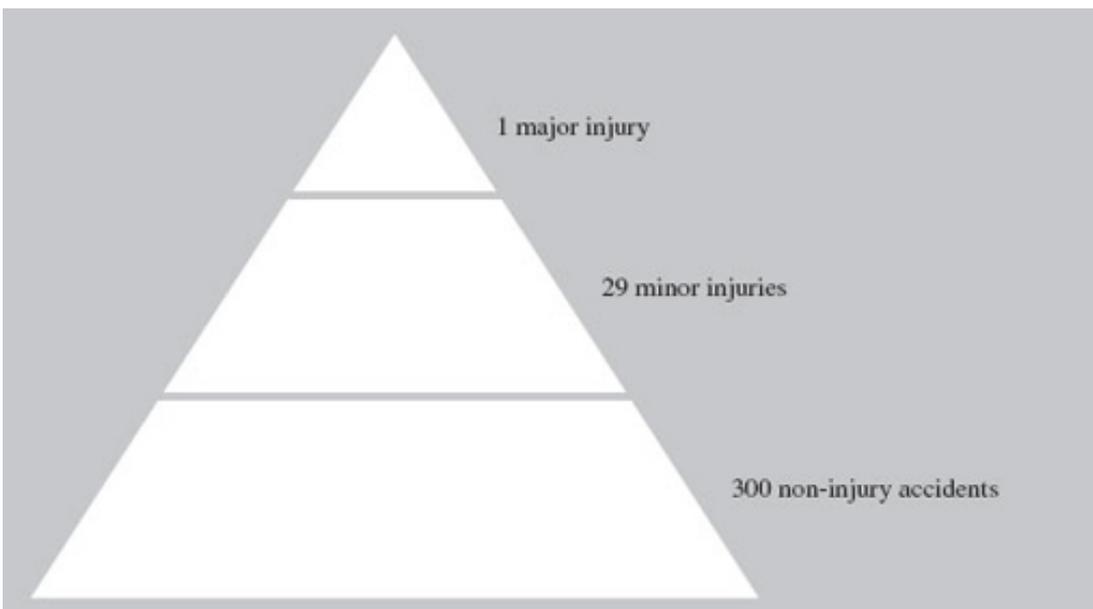


Figure 4 The accident triangle derived by Heinrich in 1931 from a study of 1500 organisations

### Activity 4

If you were setting out to repeat Heinrich's study, how might you develop this approach?

In particular, what main features would you consider in addition to those indicated in our summary of his work?

In fact many studies have followed Heinrich's approach, but they have often focused on the ratios of incidents within specific organisations. Annual reports by the Health and Safety Executive (HSE) in the UK show significant differences between industry sectors as summarised in Table 1.

In these studies by the HSE Accident Prevention Advisory Unit (APAU), non-injury accidents are defined in wider terms than in earlier studies, and include all unintended events causing loss, even when there was no potential for causing personal injury. As Table 1 shows there are marked differences between types of organisation. This study also found that the ratio of uninsured costs to insured costs was substantially greater than Heinrich's 4:1 ratio, and ranged from 8:1 to 36:1. Clearly, the mix of industrial activities, the management and training within the organisations and the definitions of accident categories have contributed to different results between the studies since Heinrich's time. Your answer to Activity 4 should have identified some of these features.

**Table 1 Accident statistics from industry sectors in the UK**

	Reportable personal injury	Other injury	Non-injury	Accidents per year
Food manufacture	1	5	148	11
Road haulage	0	1	296	14
Construction	1	56	3569	87
Oil production	1	4	126	5
Hospital	1	10	195	7

(Data extracted from HSE, 1994)

## 3 Analysing incidents

### 3.1 Types of incident

Now we can progress to an examination of some incidents by studying selected reports and publications.

Returning to the word 'accident', we can cite another definition:

An accident is an undesired event which results in physical harm and/or property damage. It usually results from a contact with a source of energy above the threshold limit of the body or structure.

(Kuhlman, 1977, p. 5)

The undesired event is again emphasised, since few of us want to suffer personal injury or damage to our property. However, businesses are built on taking chances on economic and engineering issues, while success comes from management taking chances. The challenge is balancing the chances of benefits against the chances of injury or damage. This definition also includes the critical element of contact with a source of energy above a threshold limit.

#### Activity 5

Before continuing, write down a list of types of incident involving contact with a source of energy above a threshold limit.

Your list could include some of the more obvious energy sources such as:

- contact with electricity;
- contact with heat energy (or, conversely, cold);
- contact with radiation;
- contact with noise;

but to these you could add:

- contact with chemical energy (e.g. corrosive or toxic substances).

Then there are many physical effects involving energy transfers, such as:

- falling to a lower level;
- falling at the same level;
- being struck by an object;
- striking an object;
- being caught in something;
- being caught between something.

You may be able to add more, or you may have given specific examples within these general descriptions. Whatever your list, you could probably take the line of thought further and prepare a second list of basic causes of such incidents.

### Activity 6

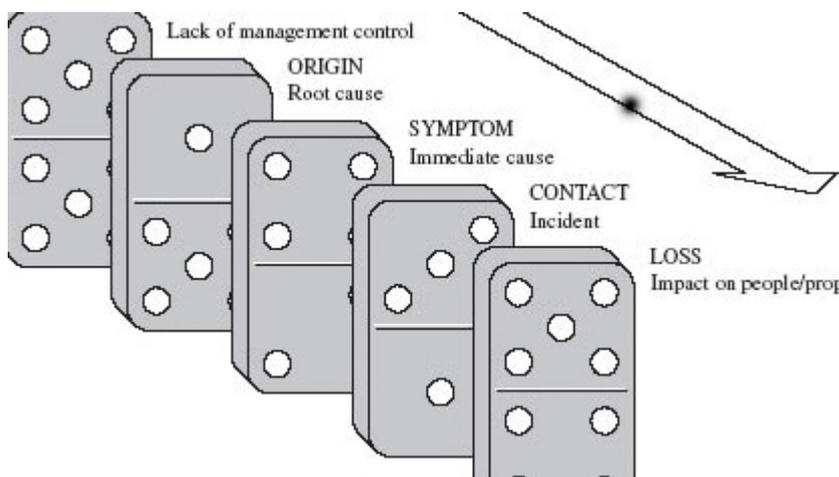
Prepare a list of causes of contact with a source of energy above a threshold limit.

Once again your list is likely to differ in detail from ours, but broadly we can consider causes as being due to unsafe conditions or unsafe practice. Our lists separated into these two categories are shown in Table 2.

**Table 2: Some causes of incidents**

Unsafe condition	Unsafe practice
Defective equipment, materials etc.	Using defective equipment
Poor housekeeping/maintenance	Operation without permission
Inadequate protective equipment/guards etc.	Rendering protective devices inoperative/not taking precautions needed
Incorrect loading/location	Operation at wrong speed
Lack of warning information	Failure to give warning
Inadequate illumination/ventilation/workspace	Fooling around

While these conditions or actions may cause an incident, they are not the root cause of it. For this we often have to look at failure of management controls relating to human factors or to job factors. So, there may be a lack of knowledge or skills among the people involved, or there may be inadequate work standards, design, maintenance and so on. The sequence has been likened to a domino effect (Figure 5). With these factors having a 'knock-on' effect, it is clear that any management system has to address possible failures at any level.



**Figure 5** The domino effect in the cause of incidents

Before contact, the aim is to prevent the causes and to detect and correct them before they can lead to incidents. So here we are concerned with engineering practice in design,

purchasing practice for materials and equipment, and work standards. While any individual may not be involved directly in these activities, it is important that communication systems allow the flow of information likely to relate to incidents.

### Activity 7

Notice that we have used the word 'incidents' rather than 'accidents' in the preceding text and activities.

Consider why we have done so.

At the contact stage the incident occurs that may or may not result in loss. This will depend on the level of energy transfer according to our previous descriptive approach. Many incidents do not result in loss. These incidents, sometimes called 'near misses', are equally important in the management process. By identifying the cause of such incidents, corrective measures may be put in place before loss does occur. Communication systems must allow the reporting of such no-loss incidents.

### 3.1.1 The cause

A small digression will be made here to question the use of the word 'cause' and to reflect on the view expressed by Kletz (1988, p. 2). He argues that the word has an air of finality about it, and is concerned that finding the cause discourages further investigation. He cites an example that the cause of a pipe failure was corrosion – which suggests that we know why the failure occurred. He draws the analogy of the cause of a fall being gravity – suggesting that nothing more can be done about it and repetition of the incident cannot be avoided. While the causal statements may be true, they must not stop further questioning:

- Was the specification of the material for the pipe correct?
- Was the specified material used in practice?
- Was the pipe used under the operating conditions assumed by the designers?
- Did the designers ask for corrosion monitoring?
- Was corrosion monitoring carried out in practice?
- What was done with the results – did action follow?

Kletz further argues that the association of cause with blame introduces an atmosphere of defensiveness. The result of this is a ready acknowledgement that an incident may have been preventable by better design or operation, but there may be reluctance to attribute it to poor design or operation.

Whatever view of the causal structure of incidents is taken, the aim should be to look beyond the immediate cause and to identify more fundamental ways of avoiding the hazard and of improving the management system, especially through attention to multiple causes and their interactions.

As a further guide, here are some questions you may consider about incidents and the identification of their causes.

- If the incident involved equipment failure, what was it that failed?
  - How can failure be prevented or made less likely to occur?
  - How can failure or its onset be detected early?

- How can failure be controlled or the consequences minimised?  
 What does the failed equipment do?  
 What can be done instead of using this equipment?
- What material was involved – leaked, decomposed, ignited, exploded ...?  
 How can such an event be prevented?  
 How can such an event or its onset be detected?  
 What is the material used for in the process?  
 Do we need to have so much of the material present at any given time?  
 What alternative materials could be used?  
 What alternative processes are available?
  - Who could have carried out their role more effectively? Look at the whole life cycle of process or product – design, construct, operate, maintain, train, inspect, etc.  
 What could they have done better?  
 How can they be helped to perform better?
  - What function is served by the operation involved in the incident?  
 Why is it done?  
 What alternatives are available?  
 How could it be done differently?  
 Who else could provide the function?  
 When can it be done?

This checklist implies that there are many ways of preventing an incident being repeated. You may also perceive the interrelationships between many of the possible causes of an incident. Now we will explore some of the general issues in assessing risk.

## 3.2 Multiple causes

Now we will explore multiple causes using an example familiar to us all – road accidents. The deaths of about 10 people each day on the UK's roads are less dramatic than, for example, the capsizing of the *Herald of Free Enterprise*, but one feature that links them both is the element of risk associated with everything we do – and even with inaction.

We have just seen that many factors contribute to the risks which result from the inherent hazards associated with something we do.

Look at the following hypothetical account of a road accident, which is not atypical of many we see in the newspapers or hear about on news bulletins:

Two vehicles were involved in an accident on the Anytown bypass late last night. X was travelling north and was in collision with another vehicle turning right from the southbound carriageway into a petrol filling station. The driver, Y, of the second vehicle and its passenger, Z, were both thrown from the vehicle, and X was taken to the Hereshire hospital in a critical condition.

A detailed investigation may conclude that a variety of factors contributed to the incident, including:

Driver X was exceeding the speed limit.

The braking behaviour of driver X's vehicle was poor.

Driver Y failed to yield right of way and turned right incorrectly.

The vehicle occupants Y and Z were not wearing seat belts.

The doors of driver Y's vehicle were not securely closed and resistant to impact.

Rain had made the surfaces wet and so reduced the coefficient of friction of vehicles on the road.

Telegraph pole and road signs were too near the road and compounded the injuries.

Driver X has a history of careless driving incidents.

and so on.

We conclude that there were many factors contributing to the cause and the severity of the incident. Figure 6, showing the effect of the four factors Environment, Engineering, Education and Enforcement (the four Es) on road accidents, is actually a very simplified multiple cause diagram, drawn from the perspective of, say, the highways engineer.

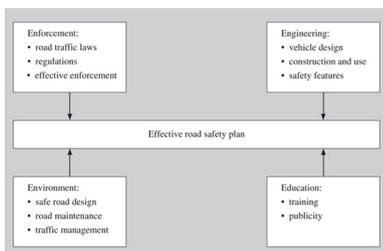


Figure 6 Elements of road safety

# 4 Integrated management

## 4.1 Introduction

Annual costs to employers from accidental injury and occupational illness are on the order of 5–10 per cent of the gross profits of UK industry. The total social cost, including the cost of benefits and National Health hospitalisation and treatment, make this a truly staggering drain on the nation's coffers!

### SAQ 2

Consider for a moment the examples of the hidden costs – the bottom of Heinrich's iceberg from [Section 2](#).

Complete Table 3 by listing examples of conventional and hidden costs. We have included some examples to start you off.

**Table 3: Examples of typical costs incurred by organisations**

Conventional costs			
<i>Initial costs</i>	<i>Operational costs</i>		<i>Final costs</i>
Site studies	Capital equipment		Closure/ decommissioning
	Materials		
	Labour		
	Supplies		
	Utilities		
	Structures		
	Salvage value		
Potentially hidden costs			
<i>Regulatory</i>	<i>Voluntary (beyond compliance)</i>	<i>Image and relationship costs</i>	<i>Contingent costs</i>
Notification	Public reporting	Corporate image	Property damage
Labelling			

### Answer

Our list is in Table 3 Completed. You may not have listed all that we have, but we hope that you have identified many of the hidden costs. If not, their significance may be even more surprising to you.

**Table 3 Completed: Examples of typical costs incurred by organisations**

<b>Conventional costs</b>			
<i>Initial costs</i>	<i>Operational costs</i>	<i>Final costs</i>	
Site studies	Capital equipment	Closure/ decommissioning	
Site preparation	Materials	Disposal of inventory	
Permits	Labour	Post-closure care	
Research and development	Supplies	Site survey	
Engineering and procurement	Utilities		
Installation	Structures		
	Salvage value		
<b>Potentially hidden costs</b>			
<i>Regulatory</i>	<i>Voluntary (beyond compliance)</i>	<i>Image and relationship costs</i>	<i>Contingent costs</i>
Notification	Public reporting	Corporate image	Future compliance costs
Labelling	Community relations	Customer relationships	Penalties/fines
Reporting	Monitoring/testing	Investor relationships	Response to future releases
Monitoring/testing	Training	Insurer relationships	Remediation
Modelling and other studies	Audits	Professional staff relationships	Property damage
Remediation	Qualifying suppliers	Manual staff relationships	Personal injury damage
Record keeping	Annual reports (public)	Supplier relationships	Legal expenses
Plans	Insurance	Lender relationships	Natural resource damages
Training	Planning	Host community relationships	Economic loss damages
Inspections	Feasibility studies	Regulator relationships	
Manifests	Remediation		
Emergency preparedness	Recycling		

Protective equipment	Environmental studies
Medical surveillance	Research and development
Environmental insurance	Habitat and wetland protection
Financial assurance	Landscaping
Pollution control	Other environmental projects
Spill response	Financial support to outside groups
Stormwater management	
Waste management	
Taxes/fees	

### 4.1.1 A hierarchy of causes

#### SAQ 3

Consider the difference between the relative safety of car and air travel in relation to the following points.

- A car travels on the ground and not at 10 000 m in the air. Compare the effects of power failure.
- A car travels at perhaps one-tenth of the speed of an aircraft, reducing the risk of injury.
- The external environment of a car can usually support life, while an aircraft is a pressure vessel designed to protect its occupants from the external environment. The integrity of this vessel may fail.
- A car carries a smaller number of passengers, and so the maximum consequences of an accident are lower compared with those of an accident to an aircraft which carries several hundred people.
- The inventory of fuel in an aircraft is far greater than in a car.

A car would appear to be inherently safer, yet statistics suggest otherwise. Rationalise this, drawing on any hard or system features to support your view.

### Answer

Taking the first point in the list, the loss of power in a car will simply make it coast to a halt, whereas an aircraft will fall from the sky. So why is travel in an aircraft safer than driving a car? This is a paraphrase of the question. In practice there are several engineering and procedural features which allow the commercial aircraft system to overcome its inherent safety disadvantages. You may have identified the following examples to illustrate this.

- There is a high level of redundancy in the critical components of an aircraft – usually two or more engines, redundant control devices, pilot and co-pilot, and so on.
- Critical components are designed and maintained to a high level of integrity. Regulations and company procedures include a high level of preventive maintenance and of inspection and testing of key components. Extensive checking of system components is done before each flight. Compare a pilot's pre-flight checklist with what most of us do when we get into a car and drive away.
- Facilities are designed to minimise the risk of collision. Compare the building restrictions around an airport with the obstacles regularly seen along roads.
- Sophisticated management systems maintain separation between aircraft both on the ground and in the air. There is no comparable traffic control on the roads.
- Like car drivers, pilots are licensed, but undergo a higher level of training, and have to undergo regular retraining. Other people involved in air transport also have to undergo extensive training.
- The extensive resources and expertise to implement the systems associated with aircraft are judged worthwhile in view of the advantages of speed that travel by air permits.

Therefore, despite the inherent disadvantages of air transport in terms of safety, it is in fact a safer means of travel.

In our response to [SAQ 3](#) it should be clear that one major difference between the two modes of travel is management systems. When the system does break down, and there is an aircraft crash, the inherent disadvantages are revealed, but extensive investigations take place to determine the cause of the incident.

Examples such as the Concorde crash, the capsizing of the *Herald of Free Enterprise*, the fire on the Piper Alpha oil installation, the fire at King's Cross underground station and various rail crashes demonstrate beyond doubt the costs of mismanaging environment, health and safety matters, as all had considerable costs both in lives and in monetary terms. All of these incidents were followed by major inquiries which revealed failures in management systems as their root cause. Table 4 gives some more simple examples.

**Table 4: Incidents that can be traced back to management**

Immediate cause	Example	Possible root cause	Possible management failure
Poor housekeeping	Employee trips over article on floor/Material falls from shelf	Hazard not recognised	Training, planning, layout
Improper use of equipment	Using side of grinding wheel rather than face, and wheel	Inadequate facilities/Lack of	Training of operators and supervisors, operating

	breaks/Use of compressed air to remove dust from surface causes eye injury	skill, knowledge, proper procedures	procedures, enforcement of procedures
Defective equipment	Electric drill without earth wire/Hammer with loose head/Vehicle with defective brakes	Lack of recognition/Poor design or selection/Poor maintenance	Training of operators and supervisors, maintenance
Procedures absent	No check for flammable mixture – explosion/No instruction to lock out power before maintenance	Omission/Error by design and by supervision	Operating procedures, training, supervision
Lack of safety device	Machine has exposed gear – severe cut/No warning horn – person hit by vehicle/No guard rail on scaffold 3 m high	Need not recognised/Inadequate availability/Deliberate act	Planning, layout, design, safety rules, equipment, awareness, motivation, training
Lack of personal protective equipment	Dermatitis because gloves or protective lotion not used/ Foot injury because materials handler not wearing safety shoes	Need not recognised/Inadequate availability	Planning, design, safety rules, awareness, training
Inattention, neglect of safe practice	Welder picks up hot metal with bare hands/Person walks under suspended load/Broken glass and spillages not cleaned up from floor	Lack of motivation/ Poor appreciation of risks	Enforcement of rules, procedures/Training, awareness, motivation

Often, preventive measures could be taken at the design and at the supervisory stage as shown in Table 5.

**Table 5: Preventive measures by design and supervision**

Cause of primary error	Preventive measures by designer	Preventive measures by supervisor
Improvisation	Provide adequate instruction	Ensure procedures supplied to person
Failure to follow correct procedure	Ensure procedure not too lengthy or cumbersome	Review procedures to ensure appropriate and not difficult
Procedures not understood	Ensure instructions easy to understand	Ensure person understands
Lack of awareness of hazards	Provide warnings, cautions and explanations in instructions	Point out precautions that must be observed
Errors of judgement, especially under stress	Minimise need for making hurried judgements, programme contingency measures	Provide instruction on action under abnormal conditions
Critical components installed incorrectly	Design components so that only correct installation possible, e.g. asymmetric configurations on mechanical and electrical connections, male and female threads on critical flow systems	Provide instruction on maintenance and repair. Ensure no change from design and do not modify a part to make it fit

Lack of suitable tools and equipment	Ensure need for special equipment minimised; provide those that are unavoidable and emphasise use in instructions	Ensure correct equipment is available and is used
Error or delay in use of controls	Avoid proximity, interference, difficult location or similarity of critical controls. Locate indicator above control so that hand making adjustment does not obscure view of indicator. Label prominently	Check equipment during selection and ensure critical controls are easily accessible, easy to select and easy to operate
Vibration and noise cause irritation and loss of effectiveness	Provide vibration isolation or eliminate noise	Where noise levels cannot be suppressed, provide ear defenders
Slipping and falling	Incorporate friction surfaces, guard rails or protective harnesses etc.	Determine where safeguards are needed to deal with hazardous locations and ensure their provision and application

You can probably add to these lists to cover other scenarios, such as irritation and loss of effectiveness through excessive heat or humidity. No matter what the organisation, management failures can be linked to risks to the organisation or to individuals.

One analysis of over 6000 incidents from 95 countries, recorded in the MHIDAS (Major Hazard Incident Data Service), identified that a release to the environment occurred in more than 50% of cases, while fire occurred in 44% and explosion in 36%. (As more than one type of incident could occur in a single accident, the total is greater than 100%.) Using a different characteristic for analysis, flammability occurred in almost 70% of cases, toxic substances in about 30%, corrosive substances in 10% and explosive substances in nearly 7% (Vilchez et al., 1995). These proportions justify the emphasis we have given in this unit to the dispersion of releases and to fire. As a result, we shall return to the all too common problem of fires to illustrate the principles in developing a hierarchy of causes of incidents.

There will always be a great temptation to view many of the incidents presented in this unit with the haughty disdain of someone with the 20/20 vision of hindsight. In some cases, it is true, the inevitability of some form of incident or breakdown was clear – the Stalybridge incident, for example, seemed to be a disaster waiting to happen. However, in other cases, the outcome of the initiating act would be far from clear at the time, especially to the people most directly involved.

### Activity 8

Many of the incidents are consequences of some quite complex chains of events – perhaps the multiple cause or domino effect introduced in [Section 3](#). A different analogy is that of a Swiss cheese in which the holes may align allowing passage through a series of barriers. This approach is described in the File Paper ‘Human error: models and management’ by James Reason, which you should now study.

Human error: models and management (PDF, 3 pages, 0.1MB)

[View document](#)

Notice that here Reason attributes active failures to the actions or inactions of operators, which are believed to cause the accident – as in the case of pilot error. Often these operators perform the last ‘unsafe acts’ that lead to unfortunate consequences. Examples

include a pilot failing to lower the landing gear before touchdown, or a surgical procedure to remove a foreign body carried out on the wrong finger rather than the finger that had the problem. In contrast, latent failures are errors committed elsewhere in the management chain. For example, overwork or stress may lead to active errors, and the resulting unsafe acts of individuals are the end result of a long chain of causes with roots elsewhere in an organisation. The problem is that these latent failures may remain dormant or undetected for long periods.

Many investigations and reports concentrate on the technical aspects of the incidents or breakdown which led to the fire or explosion. This is probably because they serve as warnings to other practitioners involved with similar materials, processes or installations, a feeling that some good must come from the disaster. There is also an unwillingness to address the more contentious issues of blame or organisational weakness, especially if death has been a consequence of the incident.

However, it is clear that in many, if not all, of the cases discussed there are underlying causes which are related less to the physical properties of materials than to the organisation of the operation, be it material, process or plant. Put more directly, the underlying cause in all cases is the failure to manage the risk.

A hierarchy of causes is shown in [Figure 7](#). At the top is the *loss* itself, that is life, property, business or the environment. The loss was caused by the incident, accident or breakdown, which in the context of this discussion is the fire or explosion. The cause of the fire is the ignition of some flammable material and the consequent development of a fire. These are the so-called *immediate causes*, in other words unsafe conditions and unsafe acts. Arson is, of course, an extreme example of an unsafe act.

Now we ask the question, 'What in turn led to those unsafe conditions, or what promoted those unsafe acts?' These are the so-called root or *basic causes*. The following is a fairly exhaustive list of these basic causes.

1. Inadequate standard of equipment.
2. Unsafe working practices – often called systems of work.
3. Poor standards of maintenance – of either equipment or systems of work.
4. Inappropriate or inadequate information.
5. Inappropriate or inadequate training.
6. Inappropriate or inadequate supervision.
7. Inappropriate or inadequate personal action.
8. Personal grievance.
9. Poor security.

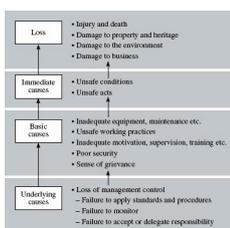


Figure 7 A hierarchy of causes

Most of these basic causes are self-explanatory; you can probably relate many of them to the comparison in SAQ 3. An example of inappropriate or inadequate personal action might be ignoring a smoking ban in a sensitive area. You might also say that smoking in a

non-smoking area is an example of inadequate training or supervision, and you would probably be right. We would simply make the point that the basic causes listed above are not independent of each other – there are very strong interactions on that list.

## 4.2 Why integrate management systems?

Integrating any management system with the business is essential if progress is to be made, but here we are concerned with integrating management systems with each other. Managing a business continues to set new challenges and demands especially when viewed against:

- significant competition;
- high customer and community expectations;
- returns on capital employed;
- regulatory compliance;
- executive liability risk.

Standards and legislation affecting health, safety, environment and quality assurance share many common elements that if effectively integrated will stimulate business improvement and risk reduction. Integration will expose areas of waste and non-value-added activity, and provide opportunities for rationalisation and/or removal of:

- documentation;
- certification audit and review procedures;
- barriers across departments or functions.

Traditionally, standards and regulatory issues have been viewed as separate and specialist facets of management. The consequence of a separate approach is that actions and decisions are made in isolation and therefore are not optimal. Employees may be presented with a proliferation of information and even conflicting instructions which may put the company at risk. Bureaucracy can flourish; how many systems can you cope with? There also tends to be lack of ownership, with inevitable problems.

Look at the following situations and note the potential conflicts.

- Carbon in an abatement system fitted to a tank vent to adsorb emissions may undergo auto-ignition and lead to a flashback to the tank, resulting in an explosion.
- Walls around equipment to improve the working environment, such as to reduce noise from a compressor house, may allow gases to accumulate with resulting inhalation or fire risks. Similarly, walls on offshore platforms may form enclosures in which gases collect causing fire and explosion risks.
- Low-lying pits, such as high bunds and pump pits to collect leaks from pump seals, may collect toxic and flammable gases with resulting dangers to personnel needing to work in such locations.
- An underground fuel tank may reduce the fire hazard but increase the uncertainty about groundwater contamination. Moving the tank above ground reverses the relative risks.

An approach to integration in the processing industries may involve evaluating the potential impacts of continuous as well as accidental releases. These consequences can

be addressed by developing an integrated approach to quality, environmental, health and safety management.

Interest in safety and health management systems grew for many reasons. The change from reactive to a proactive approach to management requires that risks should be identified and controlled before the first adverse event. Such an approach is in principle more effective, but also more challenging. Success demands the design and implementation of robust management systems that incorporate, among other things, clear policies, procedures for planning and implementing risk assessment and control, and suitable arrangements for monitoring and reviewing performance and so leading to continuous improvement.

Some people link quality, safety and environmental problems as having a common cause – entropy, a measure of the disorder or randomness in a system, from the second law of thermodynamics. Effective management systems are presented as a way to reduce entropy. Safety and environment are placed as subsets of quality and therefore responsive to a ‘quality approach’. In the mid 1990s the total quality management (TQM) concept was promoted as a suitable framework for integrating quality and safety to strengthen the management approach to safety. Major accidents such as Piper Alpha, Clapham and Kings Cross have been cited as the turning point in the realisation that strong proactive management systems are required to make any real impression on the reduction of accidents. Could the self-regulation approach of TQM and use of quality management tools bring about this change?

TQM has many strong parallels with environmental management. However, there are important differences between TQM and environmental management which mean that many quality initiatives are insufficient to deliver environmental improvement by themselves. The essence of the difference can be seen by asking the questions ‘Who is the customer?’ and ‘What is the objective?’ If the environment is the customer, then the definition of a satisfied customer becomes problematic. With TQM, an objective could be ‘zero defects’, which is relatively easy to define and measure. However, the only agreement about an objective of ‘zero environmental impacts’ may be its impossibility. We could consider breaches of environmental regulations as a possible objective. Starting with this as the comparison and widening the scope to include health and safety issues, the three dimensions may be compared as shown in Table 6.

**Table 6 Comparable features of quality, environmental and safety systems**

Quality	Environment	Safety
Goal is zero defects	Goal is zero breaches of authorisations or environmental regulations	Goal is zero accidents
Customer complaints	Community complaints	Serious injuries
Event analysis	Event analysis	Incident analysis
Documented policies, procedures and work instructions	Documented policy, procedures, work instructions, authorisations and licences	Written policies, procedures and guidelines
Quality circles, improvement teams	Environment committee, energy management team, waste reduction team, community liaison group	Safety committee
Empowerment	Employee participation	Employee participation

Control charts	Run charts, statistical analysis	Statistical analysis
All nonconformances are preventable	All emissions are preventable	All accidents are preventable
Internal audits	Environmental audit	Workplace inspections
Quality training	Environmental training and awareness	Safety training
Quality records	Environmental records, waste regulatory documents, emission records	Safety records
Design for quality	Design for environment, design for recycling, control of emissions	Design for safety

Two international standards have been developed, one for quality assurance/management (BS EN ISO 9000 series) and one for environmental management (BS EN ISO 14000 series). Both standards integrate these functions within a business management framework and address areas analogous to health and safety for which national guides have been published as described earlier. In the UK, BS 8800 embodies the philosophy and approach of *Successful Health and Safety Management* prepared by the HSE, and other authoritative texts. Current management science theories suggest that business performance is improved in all areas, including health and safety, if it is measured and continuous improvement sought in an organised manner.

### 4.2.1 Comparing the management systems

One approach to BS 8800 follows the ISO 14001 model, and the ISO 14001 system itself was closely modelled on the previous ISO 9000, with the 2000 revision of ISO 9000 following ISO 14001 principles. As a result, you may imagine that there are similarities between the standards. Many of the elements are similar, and some are nearly identical. Management systems share common elements, including developing and documenting procedures, training, record keeping, auditing, and corrective action. Figure 8 illustrates this in relation to the cycles for environment and health and safety.

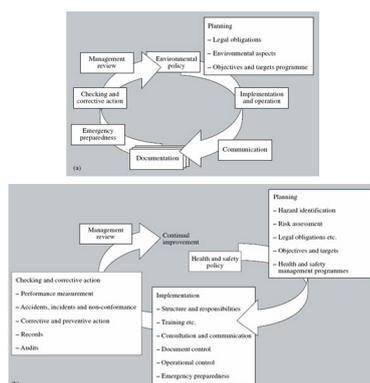


Figure 8 (a) Environmental and (b) health and safety management system cycles compared

Please click on the 'View document' link below to view a larger version of Figure 8.

[View document](#)

The foundation of ISO system standards is a TQM approach. These standards are process-oriented and are used to evaluate management systems. They do not establish technical guidelines, limits or goals. They do not measure performance.

ISO 14001 describes the basic requirements of an environmental management system. It is the standard that organisations implement and to which they either seek third-party registration or self-declaration of conformance. An ISO 14001 registration will not guarantee that a particular facility has achieved the best possible environmental performance, only that it has put an environmental management system in place. Notice also that the 'continual improvement' mentioned in the standards refers to continual improvement of the management system itself, not environmental performance directly. Most professionals agree that a systematic method is equally essential for an effective safety programme.

Quality management is based on the quality management principles listed in Table 7. These are comprehensive and fundamental rules or beliefs, aimed at continually improving the performance of an organisation over the long term by focusing on customers while addressing the needs of all other stakeholders. ISO 14001 is aimed at these, and more: 'customer requirements' expands to embrace regulatory and other mandatory environmental requirements; and 'continual improvement' is driven not only by 'customer' expectations but also by priorities and objectives generated internally by the organisation.

# 5 Emergency planning

## 5.1 Introduction

Much of this unit is about risk, but as we have seen, it is a word with different interpretations – the risk of harm, the chance of gain or simple uncertainty, for example. So it may be seen as a balance between conformance and performance in an organisation. Although functional emphasis and management boundaries are inherently flexible, risk linked to harm typically represents the perspective of managers responsible for conformance activities – particularly, the financial controller, internal audit, health and safety manager, environmental manager and insurance administrators. Risk as opportunity often reflects the outlook of senior management and the planning staff, who largely address the potential gains from risk. Risk as uncertainty is a perspective of line management responsible for operations, and as things may not turn out as expected, surprises can occur.

Emergency planning is all about preparing to cope with situations that have the potential to cause a great deal of harm. It often involves organisations who do not routinely work together, and who work in different ways, having to co-ordinate their activities to provide an integrated response. Remote rural areas and large urban areas have different needs, so even organisations with similar legal functions such as police forces, local authorities, hospitals or ambulance trusts, have differing arrangements devised to cope with local situations. This means that no single definitive plan can be proposed. Guidance documents and liaison arrangements must be flexible enough to ensure that local or special needs can be taken into account.

### Activity 9

We have suggested that emergency planning is concerned with situations with the potential to cause harm. Consider an organisation with which you are familiar and make a list of what could come under the heading of 'harm'.

As ever, your response will depend on the type of organisation you consider. What we hope is that you look wider than the more familiar forms of 'harm'. One such example would be harm to the share value of an organisation. It is widely recognised that emergency situations, and at worst catastrophes, can have a major impact on share value.

In the UK, as well as the administrative differences in areas with a single tier (Unitary) local government structure, compared to a two-tier (County and District) structure, there are variations in Scotland, Wales, Northern Ireland and the Island authorities. This may (or may not) be compounded by the creation of Regional Assemblies within England. Other EU countries and countries outside the EU will work to different systems again. To attempt to describe all these local variations would be very difficult, if not impossible. This section is therefore based on the situation in England and Wales. This in turn is broadly based on guidance from European directives, so the general principles should be reasonably widely applicable, even if details vary. Planning objectives and human needs also tend to be fairly universal, but you must be prepared to take the principles given in

this section and apply them in the light of the local situation, and any specific legislation applying to that area.

## 5.2 Why plan?

Captain James Lovell chose the title 'A successful failure' for an article on the Apollo 13 Lunar Mission. The failure was that the lunar landing was abandoned. The success was that, although an explosion blew a gaping hole in the spacecraft three-quarters of the way to the moon and knocked out the electrical systems as well as the service module's engine, the three astronauts returned safely to Earth. Can you think of a better example of the value of emergency planning?

Two features are common to all disasters:

1. no one thought that it could or would happen to them;
2. those who were prepared saved lives and livelihoods.

Without a plan there is little or no chance of an effective response. The written plan, as the clarification and record of a negotiated consensus, is the legal instrument of emergency management.

There are a number of reasons why organisations should produce, validate and maintain emergency plans. The first and most obvious is that in some cases it is a legal requirement. In addition, three distinct areas of interest can be identified:

- emergency planning as a public protection activity;
- emergency planning as an organisational management function;
- business continuity planning.

Although closely related and not mutually exclusive, each has some distinct features. These are described below.

## 5.3 Emergency planning as a formal requirement

Several pieces of legislation make the preparation of emergency plans a statutory requirement. The European Directive on the control of major accident hazards (Council of the European Union, 1996a), the 'Seveso II Directive', outlines the planning requirements for industrial sites with large inventories of hazardous substances. In the UK, the requirements of this directive have been incorporated into the Control of Major Accident Hazards Regulations (Health and Safety Executive, 1999a). If the site inventory of hazardous substances exceeds the quantities laid down in the regulations, site operators must prepare an on-site 'Major Accident Prevention Policy' document (MAPP).

Sites with very large inventories – designated 'top-tier' sites – must also prepare and submit for approval a safety report, demonstrating among other things that the company has:

- put into effect a major accident prevention policy and safety management system;
- identified the major accident hazards and taken the necessary measures to prevent accidents and to limit their consequences for humans and for the environment;
- incorporated adequate safety and reliability into the design, construction, maintenance and operation of the installation.

The 'necessary measures' to limit human and environmental consequences include the preparation of off-site emergency plans drawn up by the local authority, in conjunction with the company. In some cases there is also a requirement to inform residents in designated 'Public Information Zones' around sites of on-site activities, the sorts of emergency that might arise, and the precautions to be taken if an incident occurs.

There are a number of exclusions, such as risks from military sites, hazards created by ionising radiation, pipelines and waste disposal sites. These are mostly to avoid overlapping legislation as other directives apply. For example, radiation risks are covered by Directive 96/29 Euratom (Council of the European Union, 1996b) and implemented in the UK by the Radiation (Emergency Preparedness and Public Information) Regulations. Although based on separate legislation, the emergency planning requirements for nuclear facilities and chemical sites are broadly similar.

Emergency planning provisions are also incorporated into the licensing arrangements for sites such as major airports. The reason for emergency planning for sites covered by these legal and/or licensing requirements is quite simple. Without it, they are not allowed to operate.

## 5.4 Emergency planning as a public protection activity

Uniformed emergency services – police, fire authorities and ambulance services – and organisations such as NHS hospitals, have an obvious role in the response to civil emergencies. Local authorities have an important, although less clearly defined, role. This is based on a mixture of specific legal duties coupled to a general 'duty of care' to maintain essential services even in an emergency. Much of this section describes the work of local authority emergency planning officers (EPOs), and emergency services, but it is not written exclusively with these professional groups in mind. Many principles are transferable to other organisations.

The involvement of local authorities in emergency planning tends to vary. Emergency planning is usually a function of Unitary authorities, or where there is a two-tier local authority structure, of County Councils. However, one survey of local authorities in England, Wales and Northern Ireland revealed that in 1999, nearly 50 per cent of District (second tier) and Unitary authorities had been involved in dealing with a 'chemical incident' of some sort in that one year alone (Waterworth and Fairman, 2000, cited in Fairman et al., 2001, p. 1).

The working definition of a 'chemical incident' used by Fairman et al. (2001, p. 3) is: 'an event leading to the exposure of two or more individuals to any substance resulting in illness or potentially toxic threat to health'. That definition would exclude from the statistics near-miss incidents where there was a potential risk of exposure that did not materialise. The number of near misses remains an unknown number, but in [Section 1](#) you came across 'Heinrich's triangle' ([Figure 4](#)) that proposes that for every major injury there are 29 minor injuries and 300 non-injury accidents. The same probably holds good for major incidents. There must be a lot of potential major incidents that are narrowly avoided.

When considered as a public protection activity, what is being undertaken is management of a crisis. The event is (usually) external to the responding organisation. Their own organisational infrastructure is usually intact and functioning normally, and all their resources are accessible. This may mean that they overlook the possibility of themselves

being affected. Storms and severe flooding can make it just as difficult for emergency service personnel to get to their operational base, as to get vehicles and equipment from the base to where they are needed. Disruption to the electricity distribution system can put control rooms and public buildings such as council offices and hospitals out of action. Organisations planning to cope with an emergency affecting someone else must also plan to cope with an emergency affecting themselves – possibly occurring at the same time.

## 5.5 Emergency planning as an organisational management function

If emergency services' EPOs plan to respond to other people's emergencies, people managing a business activity with major incident potential have a different perspective. They have to respond to emergencies within their own organisation. In effect, if an incident occurs, the organisation is itself in a crisis, with functionality impaired. All of this comes into the corporate governance area and the implications of internal control. This requires companies to ensure that they have a sound system of internal control and effective risk management processes which are regularly reviewed by the board. The entire system, including risk management processes, must be specifically reviewed for effectiveness by the board at least on an annual basis. Some organisations have their own versions – as with clinical governance in the health sector.

Consider this scenario. You are having a normal day at work, when suddenly there is a huge explosion. People around you start running. Has your site been the target of a bombing, was it a gas explosion, was it a tanker collision nearby or was it from a process on your site? Whatever the cause, responding as best you can to the panic all around, you direct employees outside to what seems a safe area. Then you hear a second explosion causing more casualties. As a manager, your immediate concerns may be taking care of the injured, putting out the fires, securing the site and responding to calls from family members and the media. In the aftermath of this incident, two important questions will be asked of management and directors. Employees, the media and the public will want to know:

‘Did you take reasonable precautions to prevent an incident such as this from occurring, with the inevitable consequences?’

‘Were you prepared for such an emergency?’

The answers could have major consequences for your company, its financial position and its future.

While emergency preparedness may not be a legal obligation, nevertheless changing views of liability may regard it as negligence if you fail to plan for emergencies.

We have seen through this unit that employers are obliged to take reasonable steps to eliminate or diminish known or reasonably foreseeable risks that could cause harm. So will they be considered negligent if they do not plan for emergencies? Think of it as the common law of simple negligence but applied in a different way. The importance of risk and business continuity management was elevated following the terrorist attacks on 11 September 2001 in the USA. Organisations worldwide are now revising their assessment of terrorist risks and struggling to understand how they could survive such attacks and other disasters. The range of known hazards is widely perceived to have broadened, and organisations can now reasonably be expected to prepare for these newly foreseeable

risks. Think back to [Activity 9](#), which we presented you with at the beginning of this Section. The emergencies may not be as dramatic as an explosion, but they may have an equally devastating impact on your organisation. It could be an incident due to tampering with a product, inadequate testing of a product, a rumour that relates to your business activity or simply extreme weather conditions. So be prepared for surprises.

Emergency planning and management arrangements are elements of a number of environmental management systems standards. These were covered in [Section 4.2](#), but Table 8 outlines the main requirements. Organisations going for certification would need to prepare emergency plans as part of the application and approval process.

**Table 8 Environmental management systems – emergency preparedness requirements**

ISO 14001 (1996)	Eco-Management and Audit Scheme	OHSAS 18001 (1999)
Define and maintain procedures for responding to emergency situations	Examine and assess the effects arising from potential emergency situations	Carry out a comprehensive analysis in order to identify hazards and assess risks
Prepare procedures for preventing/mitigating environmental effects	Take measures necessary to prevent accidental emissions of material or energy	Outline controls to address the hazards and risks identified
Review applicable procedures after the event	Ensure co-operation with public authorities to minimise impacts of accidents	Establish plans and procedures for emergency situations

Even if the law does not specifically require it, emergency planning is still a core function of all managers but it is probably fair to say that many hold it in very low esteem.

### Activity 10

Why do some organisations fail to prepare for foreseeable crises? Make a list now before continuing.

Common excuses and reasons could include the following:

- ‘It can't happen here.’ It is human nature to push negative images out of our minds. In the short term, we gain comfort from this view.
- ‘Emergency preparedness isn't a priority.’ Few managers would disagree that it is best to be adequately prepared for critical incidents in the workplace, but it is not their main role, and inevitably siphons resources away from the core business. Competing priorities can be allowed to ensure that emergency planning never gets under way.
- Some individuals continue to turn a distinctly Nelsonian eye to potential emergency scenarios (during the Napoleonic wars, Admiral Horatio Nelson intentionally put his telescope to his blind eye and declared he could not see the signal ordering him to withdraw from battle). If you aren't looking for something, you generally won't find it. Unless an analysis of foreseeable risks is conducted, you probably won't be aware of the full range of risks you face, both inside your organisation and from external threats.
- Ignoring emerging warning signs. Internal history may not be critically analysed, so that near misses and obvious weaknesses are overlooked. Similarly, the risks and

disaster experiences of others in the same sector of activity or locality are not recognised as useful hints for emergency preparedness.

- Relying on weak and untested plans. Often, plans are drawn up hastily, but having them gives a false sense of security. Unless a crisis plan has been carefully constructed and thoroughly tested through simulations and emergency exercises, it will not protect your organisation effectively if a crisis happens.

Time and effort spent on emergency planning may not make an immediate contribution to profits, even though in the long term it may be essential to allow the organisation to survive a crisis.

Planning also includes measures to prevent emergencies arising or escalating. These will certainly limit the ability of managers to take short cuts or override procedures to overcome temporary difficulties in order to maintain production. Such restrictions are often seen as unnecessary nuisances – until something goes wrong! The difficulty is that people responsible for some particular task or function often end up with a degree of tunnel vision in that all they can see is the task they *must* complete at all costs. They can lose sight of the possible wider consequences of their actions. Emergency planning is not on their personal agenda. In jargon terms, the organisation lacks a ‘safety culture’.

If you feel that this claim needs to be justified, remind yourself of the Flixborough disaster of June 1974. The process being undertaken at the site involved the oxygenation of cyclohexane (a substance described as having similar properties to petrol) by heating it to 155 °C at 0.86 MPa pressure, and pumping air through it. On 27 March 1974, a 1.8 m crack appeared in one of the reactor vessels. In order to maintain production, a temporary bypass pipe was installed. This bypass pipe did not comply with the relevant British Standard, and incorporated a flexible bellows system in a way that contravened the manufacturer's design guide. Plant operation continued and 34 days later (1 June) this temporary bypass failed. A major leak was followed by an explosion, estimated to be the equivalent of between 15 and 45 tons of TNT. Twenty-eight workers were killed and 36 injured. Falling debris started fires up to 3 miles (4.8 km) away, and one piece of debris was found over 12 miles (19.3 km) from the site.

According to the inquiry report, no one appeared to consider that anything was amiss. Only one person expressed any concern at restarting the plant before finding out why the reactor cracked, and checking other reactors for similar problems. In the words of the report, no one ‘appears to have considered that (it) was anything other than a routine plumbing job’ (Parker, 1975). This disaster came at a time when current health and safety legislation was just being formulated. Lord Robens, whose committee provided the basis for the Health and Safety at Work etc. Act stated that: ‘... the main conclusion of the Robens Committee was that there was one single cause, above all else, for accidents and ill health at work. This was apathy’ (Selwyn, 2002, p. 5).

It might be argued that the experience of Flixborough would guarantee that something similar could not happen again. Unfortunately, as statistics show, that is not the case. Incidents such as the Flixborough disaster are, fortunately, rare. One drawback to using such extreme examples is that people managing smaller-scale risks tend to use the excuse like that we gave earlier: ‘It couldn't happen to us – we aren't large enough!’ Emergencies can have several harmful effects and pollution is only one of them, but the number of pollution incidents may serve to give an idea of the size of the problem. The Environment Agency (2003a) reports that in 2002 there were over 29 000 substantiated pollution incidents. There were 119 ‘major’ incidents, and 784 water pollution incidents, 458 land pollution incidents and 219 air pollution incidents where the impact was considered ‘significant’. Some 1387 events led to prosecutions resulting in fines totalling

£3.65 million, the average fine being £8744. Companies would, of course also be liable for any clean-up costs, on top of the fines. Surprisingly, just over 10 per cent of the incidents involved 'catering and hotel services, healthcare premises, schools and recreational sites' – not normally perceived as 'high-risk' locations.

Table 9 summarises some disasters that befell businesses.

**Table 9 The costs of some disasters to businesses**

Date	Company	Incident	The costs
1982	Johnson & Johnson	Product tamper and recall of 31 million bottles of Tylenol capsules (known in the UK as paracetamol) after an employee injected cyanide into some capsules, resulting in the deaths of seven people. In fact, fewer than 75 capsules were found to be poisoned. Advertising and product distribution were halted. A tamper-resistant pack was designed and the product was relaunched a few months later	In 1991 the families of the seven victims reached an out-of-court settlement with the company. The cost of the recall was estimated at \$100 million and \$50 million for business interruption losses. The company sued its insurers for \$67.4 million in 1986, but lost the case
1984	Union Carbide	Liability from the Bhopal incident	Over \$527 million
1986	Johnson & Johnson	The sale of Tylenol capsules was again suspended after a woman died of cyanide poisoning. Capsules were recalled from 14 countries	\$150 million
1986	Sandoz	Fire and pollution, Rhine	\$85 million
1987	P&O	Liability, Zeebrugge	Over \$70 million
1988	Occidental	Fire and explosions, Piper Alpha	\$1400 million
1989	Exxon	On 24 March the Exxon Valdez oil tanker ran aground, spilling 250 000 barrels, an amount equal to more than 10 million gallons, of oil into Alaska's Prince William Sound. Efforts to contain the spill were slow as was Exxon's response. The Exxon name tends to this day to be synonymous with an environmental disaster. The incident illustrates how not to respond during a crisis	The clean-up cost the company \$2500 million with \$1100 million in various settlements. A 1994 court case also fined Exxon a further \$5 billion for its recklessness, which Exxon later appealed against. In addition to the direct costs of the disaster, Exxon's image was tarnished, perhaps permanently
1990	Perrier	Product recall. Benzene carbon filters intended to remove benzene, a carcinogen, became clogged, and this went undetected for six months. No one suffered as a result of drinking the benzene-contaminated water, but Perrier was forced to recall 160 million bottles from 120 countries. There were contradictory statements from management on the extent and cause of the contamination	Eighteen months after the incident, Perrier's share of the sparkling water market declined from 13% to 9% in the US, and from 49% to less than 30% in the UK. The cost of the recall was \$263 million. The company had no product recall and guarantee insurance. The stock price fell (see <a href="#">Figure 9</a> ) and the company became a takeover target. In July 1992 it was taken over by Nestlé and 750 people in

			the mineral water division were made redundant
1992	Commercial Union	Terrorism, Baltic Exchange	\$2170 million
1993	Heineken	Defective glass, manufactured by Vereenigde Glas, was found to splinter when export beer bottles were opened or transported. The company recalled, destroyed and replaced 15.4 million bottles, warning the public of the dangers through the media. No one was injured	The estimated loss from the incident was \$50 million. In 1994, the glass manufacturer agreed to compensate Heineken for an undisclosed sum. The proactive handling of the incident by the company resulted in little initial loss of shareholder value, followed by an increase in value
1999	Coca-Cola	When more than 100 Belgian children suffered nausea and headaches after drinking Coca-Cola products, the Belgian Health Ministry ordered the withdrawal of a range of suspect soft drinks produced by the company in Belgium. A similar ban was also made in France and Holland where exports from the Belgian plants are widely sold. It was claimed that the Antwerp factory used the wrong type of carbon dioxide that imparts 'fizz', making the drink taste bad, and a fungicide had caused some contamination at its factory in northern France	Coca-Cola recalled 15 million cases of its soft drinks across Belgium, France and Luxembourg, and the company temporarily closed three factories in Europe before revealing that its sales had fallen by as much as 2%. Share prices also declined
2001	Bridgestone/ Firestone Inc./Ford	The recall of 16 million Firestone Wilderness AT tyres in August 2000 was followed in 2001 by the US Government requesting another 3.5 million Firestone tyres to be recalled for safety checks by Ford, which used them on sports utility vehicles. It was found that the treads on several models were separating from the tyres. The tyres were believed to be the cause of rollover crashes that resulted in 203 deaths and more than 700 injuries. Both companies were forced to take action	Firestone spent more than \$350 million for the recall with potentially far more in legal cases. There was also the loss in public confidence of the product. In the 2000 recall, the chief executive refused to become involved and ignored the role of public relations, following Ford's PR policy at the time. Ford then tried to force responsibility onto the tyre manufacturer. The Bridgestone share price dropped by over 50%

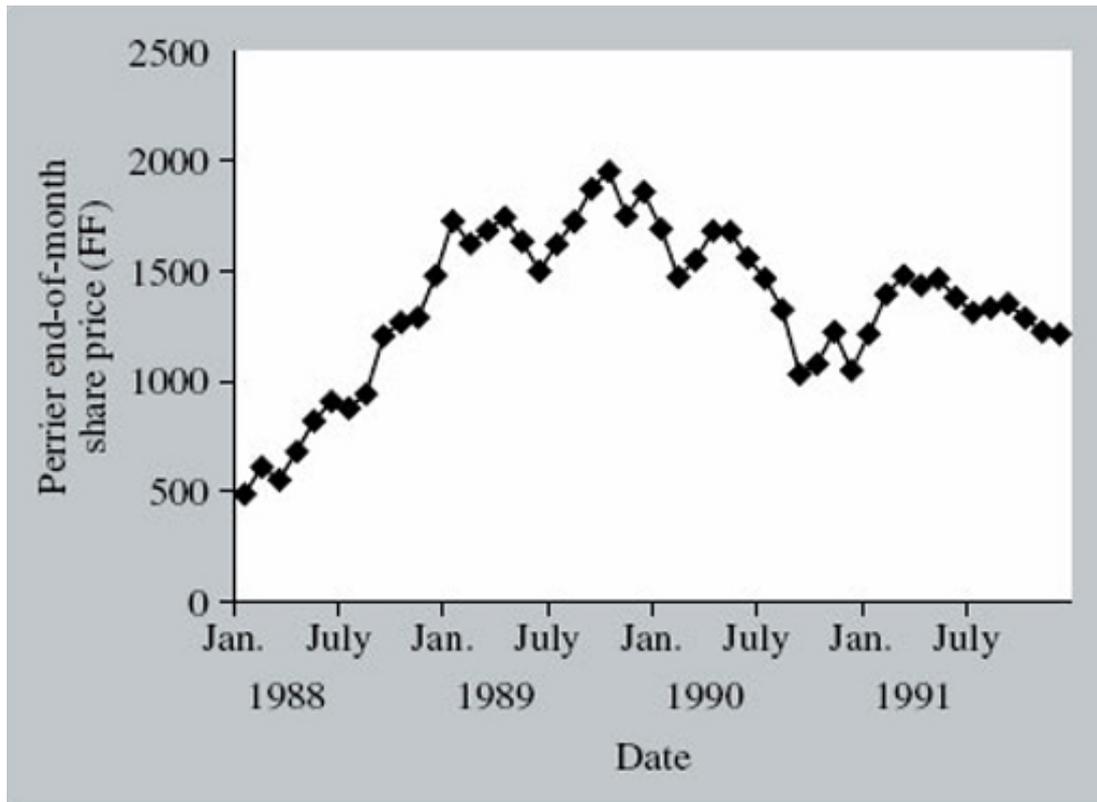


Figure 9 How an emergency can affect share price

As you may expect, initially such incidents often have a significant negative impact on shareholder value as Figure 9 illustrates. Studies have found that this fall often amounts to almost 8 per cent of shareholder value, but recovery tends to occur in 50 trading days or so. While this may suggest negligible net impact on shareholder value, the ability to recover varies considerably between organisations. Some argue that if the price falls below a threshold, recovery is impossible. The impact of such incidents on companies' share prices comes from two sources. The first is the direct financial cost of the incident in terms of cash flow, with the market adjusting the stock price accordingly. Then the market adjusts the share price in accordance with its assessment of management's handling of the incident.

There are several lessons to be learned from the incidents outlined in [Table 9](#). Johnson & Johnson's decision set a standard for incidents involving product tampering. Tylenol (paracetamol in the UK) was the first acetaminophen-based analgesic to be sold as an over-the-counter drug, and following aggressive promotion become a market leader.

## Acetaminophen

Acetaminophen belongs to the class of drugs called analgesics (pain relievers) and antipyretics (fever reducers). It relieves pain by elevating the pain threshold and reduces fever through its action on the heat-regulating centre of the brain.

Side effects of acetaminophen include yellow skin or eyes, hives, itching, bleeding (bloody urine, black stool, bruising, or pinpoint red spots), fever, sore throat, and decreased urine output.

An overdose of acetaminophen can result in liver toxicity, liver failure, and even death. The signs and symptoms of liver toxicity may not become apparent for two to three days after a

toxic overdose. Early treatment with acetylcysteine (Mucomyst) can prevent liver damage or death.

Following the product tampering, the company ordered a recall of more than 31 million bottles at a cost of more than \$100 million. It also temporarily ceased all production of capsules and replaced them with more tamper-resistant products. This drastic style of response had never before been attempted and prompted scepticism. However, the company stood by its decision. It was able to use the crisis to demonstrate to its customers its commitment to customer safety and to the quality of the product. In addition, the willingness to be open with the public and communicate with the media helped the company maintain a high level of credibility and customer trust throughout the incident. Directly following the incident, Johnson & Johnson's shares fell 7 per cent, and the company dropped from having 35 per cent to 8 per cent of the non-prescription pain-relief market. However, advertising to regain the public's trust, and an aggressive campaign to rebuild the brand emphasised a new triple-tamper-resistant package never used before. By the following spring, Johnson & Johnson had regained its previous market share. When the second incident occurred four years later, the company knew how to handle it. While this was soon identified as an isolated incident, Johnson & Johnson decided to discontinue capsule products – seeking to demonstrate its commitment to putting safety first. However, more recent debate about the product's side-effects caused more bad publicity and more costs of legal settlements, but the company was less willing to have more explicit warnings on labels.

### Box 1: Some lessons in communication

Reputation can be harmed in an instant, but it can be protected by planning for an emergency and dealing with communication issues well. In the Tylenol case the steps for doing this were as follows.

1. The first priority was designing a tamper-resistant container.
2. Johnson & Johnson strongly endorsed legislation making tampering a crime. They also urged legislators to require tamper-proof packaging for many over-the-counter drugs.
3. The company held a 30-city video teleconference from New York just six weeks after the cyanide deaths. The event was set up in only three weeks. This was remarkable for such a sensitive press conference. The chief executive spoke during the teleconference as well as other company representatives who showed the new packaging and gave every reporter a sample of the new product – a good use of visual aids for the media.
4. To overcome the public's fear of the product, the company invited former users (although they did not have to prove that they were) to call a freephone number to request a free bottle in the new packaging. The aim was to get back former customers and gain new ones irrespective of the cost.
5. A massive advertising campaign included a discount voucher for purchasing Tylenol.
6. About 50 million capsules were sent to doctors for free distribution. Patients receiving the samples would feel reassured that Tylenol was safe because doctors were demonstrating sufficient faith in the product to issue it to their own patients.

7. The company thanked the media for fair coverage and thanked them for reporting the news of the cyanide deaths to make the public aware of the problem. In contrast, treating the media as the enemy encourages probing by reporters who believe there is something to hide.

By using television and newspapers to warn people about the recalled Tylenol, the company was treated fairly by the media for being open and honest about the problem.

Timeliness is a major factor in any emergency situation, and Exxon failed to recognise this. Since the Johnson & Johnson incident in 1982, a company was expected to deal with the actual problem well – in this case, cleaning up millions of gallons of spilled oil. In addition, a company must create a positive image of how the problem is handled.

So there are several lessons to learn. Communication with stakeholders is essential, and should take account of the cardinal rules of risk communication. Prompt action is also essential, and if this involves disclosing information, it is preferable to disclose early rather than to do so after pressure, which may suggest you have something to hide.

Also important is the liaison between people involved with emergency preparedness in the organisation and those in the emergency services.

## 5.6 Business continuity planning

An organisation's strategy regarding insurance for its business risks is no substitute for high-quality risk management and emergency preparedness to address all contingencies. Some incidents we have mentioned above. Others may involve IT security for example. While the day-to-day activity of an organisation may not be particularly hazardous, it can still be affected by a hazard not of its own making. Examples might be a natural disaster such as flooding, or a hazardous activity on an adjacent site. Unfortunately, in today's society commercial undertakings or places where people gather can also be a target for terrorist activity. One strange twist is the targeting of catering outlets as they are places where people congregate. Also, some fast-food outlets are regarded as being 'legitimate' targets because they are perceived as a symbol of western capitalism. The risk was highlighted in an article in a trade journal with the rather attention-grabbing headline: 'Spy chief warns food industry over terrorism' (Anon, 2003, p. 2). The article reported that 'in a rare move' the head of MI5 had issued a warning to the food and chemical industry that it was vulnerable to a possible terrorist attack as it posed 'a very attractive target'. The changing nature of terrorism resulted in threats to new industrial sectors. As a result, police had been advising food manufacturers and distributors about security measures to help prevent a terrorist poisoning of food supplies. Should such an attack ever take place, or more importantly should an attack ever be claimed to have taken place, effective emergency planning would be essential. There would be an urgent need for an effective food recall system to withdraw suspect food from sale, and warn the public. You will have noticed from [Table 9](#) that tampering with products has caused significant loss to companies in the past.

Of increasing concern is the risk of what is euphemistically referred to as 'collateral damage', where an organisation might be affected by terrorist activity aimed primarily at some nearby target. This was a major feature of terrorist attacks on the city of London, particularly the St Mary Axe bomb (April 1992) and the Bishopsgate bomb (April 1993). Similar problems were experienced after the Canary Wharf bomb (February 1996) and the Manchester city centre bomb (June 1996).

St Mary Axe is a street in the City of London, near the Baltic Exchange. On 10 April 1992, a terrorist bomb hidden in a transit van exploded. Three people were killed and about 130 injured. The bomb left a crater about 4.3 m deep and 4.5 m in diameter. One 2 m piece of debris was blasted over 600 m, and part of the vehicle was found on the seventh floor of the NatWest Tower. The ground shock was felt 13 km away.

One organisation affected was the Commercial Union insurance company. Their 23-storey office block (the St Helens building) lost every one of its windows. Fortunately, they had effective business continuity plans in place and their response to the incident is an example of good emergency planning practice. The Commercial Union response is summarised in the following information box.

### Box 2: Crisis – a timetable for recovery

Following a bomb blast at 21.20 in the City of London on Friday 10 April 1992, Commercial Union activated its disaster recovery plan within three hours. All communication links, including the telephone switchboard for the entire London area, had been lost.

At 07.30 the next morning there was a crisis meeting of directors and senior managers at which four prime considerations were identified:

- How to reinstate telephone links for 3600 extensions in the London area offices by Monday morning.
- How to accommodate 650 staff.
- How to provide them with necessary telephones, furniture and computers.
- How to inform customers and intermediaries about arrangements for Monday morning.

By 10.00, the crisis team had, by reference to the disaster plan, established:

- that the switchboard could be reconstituted at their computer centre near Croydon;
- that data requirements could be met by linking the mainframe to new screens in new locations;
- contact with telecommunications and information technology suppliers to reinstate communication and order extra equipment;
- the need to ‘cascade’ information down through the organisation, so that all 650 staff would have the facts and know what was expected of them on Monday morning;
- staff numbers in each business area and the amount of in-house office space in and around London;
- that market requirements meant that certain staff had to be relocated within the City straight away;
- that, as an investment house as well as an insurance company, a replacement trading floor would be needed by Monday morning.

On Monday 13 April, the national press carried adverts confirming ‘business as usual’.

On Tuesday 14 April, 631 of the 650 staff were working as usual. The remainder were either working from home or on holiday. The Annual General Meeting of the company was due to be held on this day.

At the appointed time for the AGM, the date and time of which had been fixed in advance, a quorum of shareholders met as close to the original venue as deemed safe by the police and passed a resolution to reconvene at the new venue.

At 14.00 on 14 April, the AGM was held 'as though nothing had happened'.

(Source: Commercial Union Risk Management Ltd)

Insurers and their loss adjusters now expect organisations to have taken appropriate actions to protect themselves against foreseeable hazards. So do other stakeholders, and especially shareholders.

Unfortunately, the threat from terrorism is now regarded as foreseeable. A survey covering 421 organisations from a broad spectrum of business service sectors, dispersed evenly throughout the UK, was conducted in 1993, the year after the St Mary Axe bomb. This looked at how the organisation would cope if they no longer had access to their computerised information systems. This survey found that 43 per cent of responding organisations still had no contingency plans at all (IBM, 1993). Reliance on computerised systems has, of course, increased enormously since then. Also, many 'business critical' applications are now held on desktop machines that even a comparatively small emergency such as an office fire may render inaccessible.

In some cases the need to plan might be an administrative requirement, for example one imposed by insurers as a condition of providing cover. In other cases it might simply be sound business sense. As official guidance notes:

Many businesses fail as a result of various types of major emergency – storm, flood, fire, terrorism, product contamination or pressure group activity. Experience shows that those businesses which have considered potential hazards and prepared response plans, which often need be no more than a few pages in length, have a much greater chance of surviving than those who are unprepared.

(Cabinet Office, 2003, p. 13)

## 5.7 Emergency planning – the process

Usually, when emergency plans are prepared the hazards already exist, and may have been there for some time. The liquefied petroleum gas (LPG) stores in the middle of many cities are a classic example. They 'grew' in the former coal yards adjacent to railways. Their presence may be accepted, whereas a new development with similar hazard potential might give rise to objections.

In the preparation of plans, the phenomenon known as 'agenda setting' must be taken into account. This is where the planning process suddenly makes people aware of a hazard that they previously were not concerned about. If conducted with an air of secrecy, emergency planning can be perceived as evidence that a special problem exists, rather than reassurance that effective safety precautions are being taken. If the public once gets the impression that things are being kept from them, be prepared for the following reactions:

NIMBY – Not In My Back Yard!

BANANA – Build Absolutely Nothing Anywhere Near Anyone!

## LULU – Locally Unacceptable Land Use!

In many ways, good emergency planning is little more than the logical application of common sense, albeit in a more formal way and on a larger scale. There is more than one way to approach the planning process, but it is usually easier to manage if it is broken down into a number of steps or stages.

### 5.7.1 Plan preparation

Perhaps the first question to ask is ‘What is an emergency plan?’ Dodswell, in his guide to business continuity management, defined an ‘emergency management plan’ as simply:

A plan which supports the emergency management team by providing them with information and guidelines.

(Dodswell, 2000, p. 56)

Another definition, of an ‘emergency preparedness plan’ prepared in the context of chemical incidents, and therefore site-specific, is:

A formal written plan which, on the basis of identified potential accidents together with their consequences, describes how such accidents and their consequences should be handled, either on-site or off-site.

(OECD, 2003, p. 178)

Widen the scope a little and make it cover ‘potential hazards’ to be handled ‘wherever they occur’, and the same definition might apply to local authority emergency planning. As with any complex process, the procedure may be broken down into a series of more manageable tasks or steps which we will now outline.

#### **Step 1: Develop emergency management policy**

The first step is that the organisation must recognise the need for a contingency plan. Then someone or some organisation has to be given the authority and resources to undertake the task. It is crucial that roles and responsibilities are clearly understood at this stage. To be effective, they have to be negotiated at the highest (strategic) level before being implemented. When developing policy, the following factors have to be considered:

- the nature of the hazards, community and environment covered by the policy;
- legislative and organisational responsibilities;
- existing related policies;
- public attitudes, expectations and perception of risk;
- resource limitations;
- the rights of individuals;
- accepted emergency management concepts.

Policies must take health and safety issues into account when considering how emergencies will be handled. There is still the need for risk assessments before personnel are committed. Welfare measures also need to be considered. Official guidance reminds us that plans must include the physical and psychological welfare of responders and the need for stress reduction measures (Cabinet Office, 2003).

#### **Step 2: Identify stakeholders**

Everyone who has an interest – a ‘stakeholder’ – must be identified and given the opportunity to take part in developing and clarifying a policy.

### Activity 11

For an organisation with which you are familiar (it could be your workplace, or an organisation with which you are involved), list the groups you would have to invite to discuss the need for an emergency plan.

Your list may have included client groups, community groups, industry groups, members of the public, politicians, public and private sector organisations, and staff. In the exercise of civil protection planning, the list of stakeholders is infinite and usually a cascade system is used to consult appropriate bodies. The OECD (2003) illustrates the range of potential stakeholders, shown in Figure 10.



Figure 10 Guiding Principles

### Step 3: Assess vulnerability

Hazards can include technological, social and health risks as well as ‘natural’ ones. A power cut no longer means simply lack of light, heat or the means to cook food. Communities, businesses and governments are now vulnerable because of their reliance on computers for the electronic transfer of information, data and money and for the control

of safety systems. Vulnerability assessment is much the same process as any risk assessment, although it may be necessary to stand back and consider wider consequences and on a larger scale. It involves asking four simple questions about risks:

- From what? (What hazards exist?)
- Of what? (What harm might be caused?)
- To what? (Who or what can be harmed?)
- So what? (The scale of possible consequences.)

### Activity 12

- Identify the hazards that could affect your organisation.
- Decide on the level of the associated risks.  
What would the consequences be if no action were taken?

Your results will obviously depend on the organisation, but by carrying out this activity you have taken an important step in preparing your emergency plan.

#### **Step 4: Select emergency management strategies**

This step involves the application of appropriate knowledge, problem-solving and decision-making skills to:

- determine emergency management situations and issues;
- identify possible strategies;
- determine criteria for selecting the strategies to be adopted.

The plan is not – or should not be – an instruction manual or a set of ‘standing orders’ on what to do. People called upon to manage an emergency are usually the same people who cope with the day-to-day running of the organisation. If the plan draws up a set of rigid emergency procedures that override normal management processes, the chances of managers implementing it are remote. Instead, the plan is, or should be, a guidance document advising and reminding the managers of agreements reached over actions and responsibilities. Where decisions or choices must be made quickly, it is a guide to which are the preferred options.

For example, if there is a fire at a chemical plant, the local authority may have to set up a temporary reception centre for people evacuated from the area at risk. There may be several buildings that might be used, and the plan might say which one to choose.

The site may have several entrances. The plan might identify which are the first and second choices of gatehouse to use as the incident control point.

In some cases the person preparing the plan might also be the manager who would have to manage the emergency. More usually, the two roles would be separate. If so, it is important that the planner does not make arbitrary operational decisions. The most effective planning process is where the manager is able to work through the operational issues, and decide on the most effective strategies when not under pressure. The planner then checks that they do not conflict with strategies devised by other managers or, if it is a generic plan that is being produced, with other stakeholders.

### Activity 13

Develop a flow chart that illustrates the structure of your organisation's response to an emergency. Identify the links with external bodies.

#### **Step 5: Develop agreed strategies into a plan**

This is the process of taking the inputs from the stakeholders derived from step 4, and turning them into the plan document. It involves developing a practical plan from the strategy. This may be circulated in draft form in order to identify and solve potential problems of implementation.

At this stage, administrative aspects need to be considered. These may include financial aspects such as call-out and standby payments or special authority to incur expenditure without recourse to normal approval or tendering procedures.

One key decision is to identify the circumstances that will activate the plan and how the appropriate level of response will be initiated. On-site and emergency service plans may be able to rely on staff on duty, at least in the initial stages. In many cases, however, it may be necessary to call out personnel from home. This is considered in more detail a little later.

It is worth repeating that plans must always be implemented with due regard for occupational health and safety. Anyone who has been on a first aid course will know that the primary rule in helping a casualty is not to put yourself in danger and create two casualties.

*The final outcome from step 5 should be a draft copy of the plan itself.*

### 5.3.2 Plan auditing

Having got the draft plan, it is worth checking it over to see that all the major issues have been covered. The appendix below contains a set of guidelines for the initial audit of a generic 'general purpose' plan. For site-specific plans such as might be produced by an SHE manager in industry, or a business continuity manager for an office complex, the headings may need some modification.

Guidelines for an emergency response plan audit (PDF, 2 pages, 0.1MB)

[View document](#)

### 5.3.3 Training, education, testing and validation

An audited plan has not been proved to work. It has simply been checked for major omissions. The next stages are to train people in the plan's contents and procedures, and to validate the plan. The relationship between 'training and education' and 'plan validation and testing' is a bit ambiguous. It could be argued that it is not worth putting a lot of resources into training until the plan has been validated. On the other hand, a plan cannot be properly validated unless the people validating it are familiar with the contents. It is a bit like the perennial argument about which comes first, the chicken or the egg! The answer is possibly that training the validation team should be regarded as a pilot exercise. They then validate the plan, and once any essential changes have been made, the rest of the workforce is trained.

### 5.3.4 Plan testing and validation

It is one thing to have a plan; it is another thing to have a plan that you can rely on to work. There is an old military maxim that 'A plan only gets you into first contact with the enemy. After that, you fly by the seat of your pants' (Anon). A 1993 IBM report on business continuity planning confirmed this when it revealed that 'half of the plans failed completely or substantially when they were first tested' (IBM, 1993, p. 5).

The IBM report identified three categories of plans:

- viable plans – tested within the last year, and proved to work;
- doubtful plans – tested, but not in the last 12 months;
- untested plans.

Of course, the ultimate test of a plan is to attempt to use it to manage a real emergency. It is a thorough test, but that is not the time to find out that your plan has left you flying by the seat of your pants!

According to official guidance:

The most effective way to validate the effectiveness of plans (other than real events) is to test and review them regularly. Exercises are a key mechanism for achieving this: to assess the arrangements properly and then to update the plans as appropriate in the light of the experience.

(Cabinet Office, 2003, p. 68)

## Conclusion

---

Perhaps it is a truism to say that all life is full of risk. We encounter many uncalculated outcomes, some beneficial and others adverse. It can be difficult to know which adverse events will prove permanently disadvantageous, since some may lead to innovation and opportunities for the future. Businesses, especially in the financial context, often consider risk in terms of opportunities for gain. Risk in our context is a way of describing the probability and consequences of harm, or at worst a disaster. Risk tries to identify the expected losses from the impact of a given threat to a given vulnerable element over a specified time period.

As a formal intellectual discipline, risk management is still evolving. Explicit techniques have been around for many years in some fields, such as engineering where deterministic outcomes are possible, i.e. where the behaviour of the system may be modelled according to some physical or chemical laws. The codes of practice developed for these relatively simple risk situations have led to many improvements in society – buildings that stay standing after earthquakes, affordable cars, etc. At a different level of complexity, the business world has developed its own practices that draw on risk methods for financial management. There are also examples in the biological and health fields.

It was not until the 1960s when military and space requirements became increasingly demanding that risk analysis was formalised into a practical discipline to deal with complicated situations. At that point, attention moved from failure analysis of individual components, to integrated assessments of the reliability of whole complex systems. Modelling techniques became formalised, methods were developed to identify and improve the weakest links, and risk management gained credibility in many industries.

Risk management involves a multitude of actors and stakeholders. In recent years, risk techniques have evolved still further to encompass human interaction with engineering systems, i.e. to combine predictable, quantifiable, technical risks with the uncertain reactions of human operators or natural systems. Management systems evolved to provide support in dealing with factors such as 'oversight'. They offer tools for the systematic implementation of policy and strategy. Integrated management systems help ensure that safety, quality, environmental and business risks are managed right across an organisation. They provide a foundation on which to build a more effective management system and create internal mechanisms for continual improvement.

Risk assessment and management are information-intensive. Large volumes of technical information have to be gathered, processed, analysed, and eventually communicated to a broad range of users under quite different conditions, ranging from planning and regulatory activities to emergency management.

An integral part of management systems is emergency preparedness – the management of emergencies and disasters.

There cannot be many organisations of any size whose activities do not involve the need for emergency planning. After studying this unit you should be in no doubt that it should be on your personal agenda. You should also appreciate the value of incorporating the process of integrated emergency management into the culture of your organisation.

One word of caution – you are now in the situation of knowing that you should have an emergency plan, and, as we understand the law, if you know that something should be done and you choose to do nothing about it then you are liable. The phrase '*noblesse*

*oblige* is usually translated as 'nobility has its obligations'. If nobility has its obligations, then so do emergency planning, and safety, health and environmental management.

# Keep on learning

---



## Study another free course

There are more than **800 courses on OpenLearn** for you to choose from on a range of subjects.

Find out more about all our [free courses](#).

## Take your studies further

Find out more about studying with The Open University by [visiting our online prospectus](#).

If you are new to university study, you may be interested in our [Access Courses](#) or [Certificates](#).

## What's new from OpenLearn?

[Sign up to our newsletter](#) or view a sample.

For reference, full URLs to pages listed above:

OpenLearn – [www.open.edu/openlearn/free-courses](http://www.open.edu/openlearn/free-courses)

Visiting our online prospectus – [www.open.ac.uk/courses](http://www.open.ac.uk/courses)

Access Courses – [www.open.ac.uk/courses/do-it/access](http://www.open.ac.uk/courses/do-it/access)

Certificates – [www.open.ac.uk/courses/certificates-he](http://www.open.ac.uk/courses/certificates-he)

Newsletter –

[www.open.edu/openlearn/about-openlearn/subscribe-the-openlearn-newsletter](http://www.open.edu/openlearn/about-openlearn/subscribe-the-openlearn-newsletter)

## References

---

Anon. (2003) 'Spy chief warns food industry over terrorism', *Environmental Health News*, 24 October 2003, p. 2.

- Cabinet Office (2003) *Dealing with Disaster*, revised 3rd edn, Civil Contingencies Secretariat.
- Commercial Union Risk Management Ltd (1992) 'Crisis: A timetable for recovery'.
- Dodswell, B. (2000) *A Guide to Business Continuity Management*, Leicester, Perpetuity Press Ltd.
- The Engineering Council (1993) *Guidelines on Risk Issues*, London.
- Fairman, R., Murray, V., Kirkwood, A. and Saunders, P. (2001) *Chemical Incident Management for Local Authority Environmental Health Practitioners*, London, Medical Toxicology Unit, Guy's & St Thomas' Hospital Trust, Chemical Incident Management Series, The Stationery Office.
- Heinrich, H.W. (1990) *Industrial Accident Prevention: A Safety Management Approach*, 5th edn, New York, McGraw-Hill.
- IBM United Kingdom Ltd (1993) *Up the Creek? The Business Perils of Computer Failure*, Loughborough and Basingstoke, IBM Business Recovery Services (IBM, in association with Loughborough University and the Computing Services Association).
- Kuhlman, R.L. (1977) *Professional Accident Investigation*, Loganville, Georgia, Institute Press (A Division of International Loss Control Institute).
- Kletz, T. (1988) *Learning from Accidents in Industry*, London, Butterworths.
- OECD (2003) *OECD Guiding Principles for Chemical Accident Prevention Preparedness and Response*, 2nd edn, Paris, Organisation for Economic Co-operation and Development Series on Chemical Accidents, No. 10, OECD Environment, Health and Safety Publications.
- Parker, R.J. (1975) *The Flixborough Disaster – Report of the Court of Inquiry (Chairman, Roger Jocelyn Parker QC)*, London, HMSO.
- Selwyn, N. (2002) *The Law of Health and Safety at Work 2002/2003*, London, Cramer.
- Vilchez, J.A., Sevilla, S., Montiel, H. and Casal, J. (1995) 'Historical analysis of accidents in chemical plants and in the transportation of hazardous materials', *Journal of Loss Prevention in the Process Industries*, 8 (2), pp. 87–96.

---

## Acknowledgements

---

Except for third party materials and otherwise stated (see [terms and conditions](#)), this content is made available under a

[Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence](#)

Course image: [Leucippus](#) in Flickr made available under [Creative Commons Attribution-NonCommercial 2.0 Licence](#).

Table 4 Hammer, W. (1981), 'Occupational Safety Management and Engineering', second edition © 1981, by Prentice-Hall Inc;

Table 5 Hammer, W. (1981), 'Occupational Safety Management and Engineering', second edition © 1981, by Prentice-Hall Inc.

Box 1 'Crisis – a timetable for recovery', 1992, Commercial Union risk Management Limited;

Activity 8 Reading Reason, J. (2000), 'Human error: models and management', *British Medical Journal*, 320, March 18 2000. © 2000, BMJ Publishing Group Ltd.

[Alessandro Cani](#) [Details correct as of 28 March 2011]

**Don't miss out:**

If reading this text has inspired you to learn more, you may be interested in joining the millions of people who discover our free learning resources and qualifications by visiting The Open University - [www.open.edu/openlearn/free-courses](http://www.open.edu/openlearn/free-courses)