

COUNTING THE COST

Managing risk,
insurance and
terrorism



ASSOCIATION OF
CHIEF POLICE OFFICERS



produced

NaCTSO

National Counter Terrorism Security Office

NaCTSO wishes to acknowledge the contributions made by many individuals associated with the following organisations:

Home Office: The Home Office is the lead government department for immigration and passports, drugs policy, crime, counter-terrorism and police.

NaCTSO: The National Counter Terrorism Security Office (NaCTSO) is a police unit co-located with the Centre for the Protection of the National Infrastructure (CPNI). We are funded by and report to the Association of Chief Police Officers (ACPO).

NaCTSO contributes to the UK government's counter-terrorism strategy (CONTEST) by supporting the Protect and Prepare strands of that strategy. We also provide guidance in relation to business continuity, designing out vehicle-borne terrorism, the protection of crowded places and reducing opportunities for terrorism through environmental design.

NaCTSO trains, tasks and co-ordinates a nationwide network of centrally-funded specialist police advisers called counter-terrorism security advisors (CTSAs). All police forces in the UK have CTSAs who provide help, advice and guidance on all aspects of counter-terrorism and protective security across a variety of business and industry sectors.

London First: London First's mission is to make London the best city in the world in which to do business. We aim to influence national and local government policies and investment decisions to support London's global competitiveness. A successful London is vital to the health of the UK economy.

Our influence is built upon the breadth, depth and calibre of our business membership, who collectively represent over a quarter of London's GDP. Our credibility comes from our informed, in-depth policy development, supported by proactive and creative campaigning, as well as from our record of achievement. We innovate, developing practical and timely solutions to London's strategic challenges. We also provide our members with an effective conduit for communication with government and a voice in the public arena.

Introduction



Terrorism and other critical events, whatever their source or form, will always have social and economic consequences. This is why it is important that businesses consider how they can prevent, handle and recover from an attack, which usually arrives swiftly and unannounced.

The plans that you put in place to help you manage the risks involved can be both immediate and longer-term. Managing these risks effectively can help you to keep your business trading.

What is this guide about?

Counting the cost provides guidance and information that will help you, as a business, to protect yourself.

It will enable you to:

- risk-assess the security and resilience needs of your business;
- recognise threats and hazards; and
- understand better the role of insurance.

This guide also includes clear diagrams, easy-to-follow step-by-step help, links to useful websites and checklists. All of these will aid you in identifying your security and resilience needs.

How to use this guide

The information contained here is primarily for small and medium-sized businesses. However, it is also relevant to businesses of all sizes. You can read the entire booklet in order to cover all the important areas in a systematic way, or you can go to specific sections if you need information on a particular topic.

More help

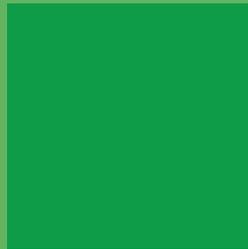
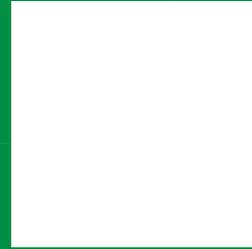
Reading this guide in conjunction with its two sister documents – *Expecting the unexpected* and *Secure in the knowledge* – will give you the basic knowledge and skills required to protect your business.

You may also wish to read the National Counter Terrorism Security Office (NaCTSO) security guides, which we have produced for some business sectors.

You can download all these guides, free of charge, from www.nactso.gov.uk

If you would like more information about the threat the UK faces from international terrorism, visit www.mi5.gov.uk

Risk



What is risk?

Risk is the combination of the probability of an event occurring and its consequences.

Of all the risks that can impact upon your business, terrorism can be particularly damaging, because it has an immediate and severe effect on many aspects of a business.

An act of terrorism is likely to impact upon:

- people
- buildings
- information
- tangible and intangible assets
- reputation
- revenue
- customers and suppliers.

The immediate and longer-term effects on a business will have financial implications when it returns to a **new normality**.

New normality is a term that is used to describe the situation that results after a critical incident. It follows the notion that the event itself will generate a new set of circumstances which changes the world as we know it. As a result, an organisation needs to review this new environment for changed, new and emerging risks that have resulted.



DID YOU KNOW?

International Standards ISO 22301 Societal Business Management Security Systems and Guidance provides further guidance on the subject of Business Continuity Plans to help businesses prepare for serious disruptions, whatever their cause. It ensures that you have the right systems and processes in place to be resilient in the face of threat.

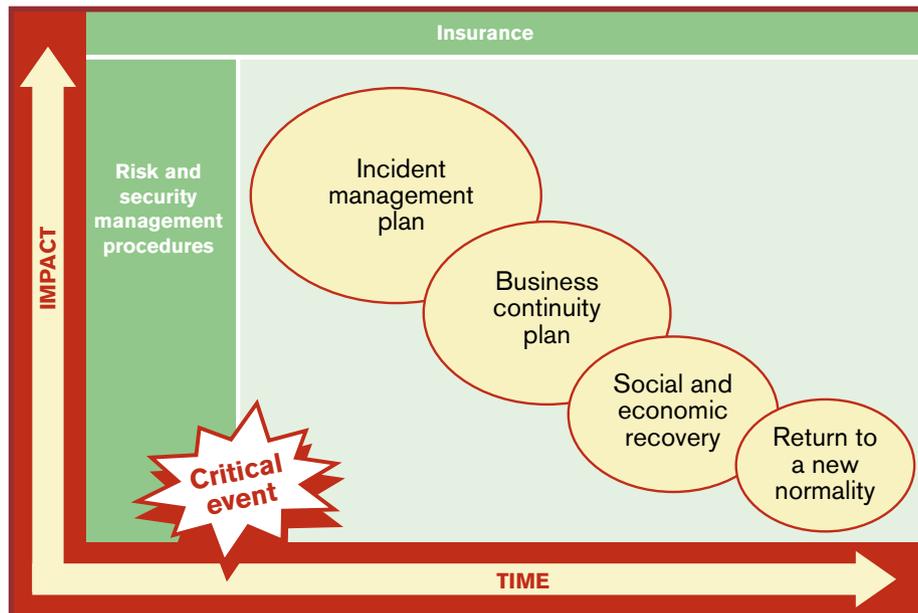
Developing and implementing a BCM response', will enable you to develop an incident management plan (IMP) the better to manage the immediate situation as it evolves. All businesses should have an IMP.

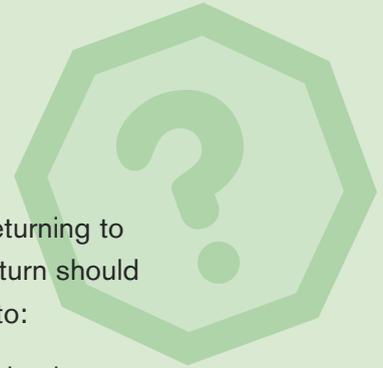
Managing risk

Risk and security management procedures are designed to protect a business from threats and hazards. Should these procedures fail, then the IMP will help businesses to manage the acute phase of the event.

The business continuity plan can be invoked quickly to protect the critical systems and assets of the business. Then a social and economic recovery stage leads on to a return to a new normality.

This process is shown in the diagram below.





DID YOU KNOW?

After a critical event such as a terrorist attack, returning to normal as soon as practicable is vital. But the return should be to a new normality that recognises the need to:

- review existing threats and hazards to the business;
- take account of new and emerging threats and hazards;
- deal with the vulnerabilities that were exploited; and
- review the actions required to prevent similar occurrences in the future.

Evaluating risk

Risks can be acceptable or unacceptable depending upon their likely impact on a business. This, in conjunction with a business's appetite for risk, largely determines whether a business will choose to manage rather than respond to risks.

Risks have two important dimensions: likelihood and impact.

- The likelihood refers to the probability of an event occurring.
- The impact refers to the degree of disruption the event visits upon a business.

In broad terms, a business should try to have ownership of the acceptable risks and seek to reduce or remove unacceptable risks. In circumstances where you cannot effectively deal with an unacceptable risk, it may remain and become a **residual risk**. It should not be ignored, however.

Following a critical event there will be a return to a new normality. This will require you to reassess the vulnerabilities and financial exposure of your business.

Counting the cost

When considering the financial impact of a terrorist attack on your business, it is useful to try to calculate your financial exposure.

As well as the value of lost equipment, you will need to factor in the cost of getting your business back to its pre-event trading position (reinstatement costs).

These reinstatement costs could include:

- undertaking repairs;
- relocating staff;
- obtaining new stock; and
- replacing IT equipment.

It is important to bear these in mind when trying to assess the impact of a critical event on your business.

So your full financial exposure would look like this:


$$\begin{aligned} & \text{Lost value} \\ & \text{of asset} \\ & + \\ & \text{Reinstatement} \\ & \text{costs} \\ \hline & = \text{FINANCIAL} \\ & \text{EXPOSURE} \end{aligned}$$

Understanding risk

Sometimes we are forced to make decisions under uncertain circumstances in all aspects of our lives, not just in business. These decisions have to be made without possession of all the facts or the ability to divine them.

As a result, it is possible to decide on a course of action from which negative consequences can follow. If a situation like this occurs, you will need to manage these negative consequences.

Risk management is both useful and important here, because it identifies these possible negative consequences and:

- allows your business to identify its critical assets and processes;
- uncovers the vital elements of cost, performance and timetables, allowing activity to be focused where it would be most beneficial to your business; and
- allows you to take some degree of control over uncertain conditions that may negatively impact upon your business.

Managing risks should follow a process as shown opposite.



The risk register

A risk register holds the key to understanding the risks that can impact upon a business. It is a central store of all risk records and associated information, and should include:

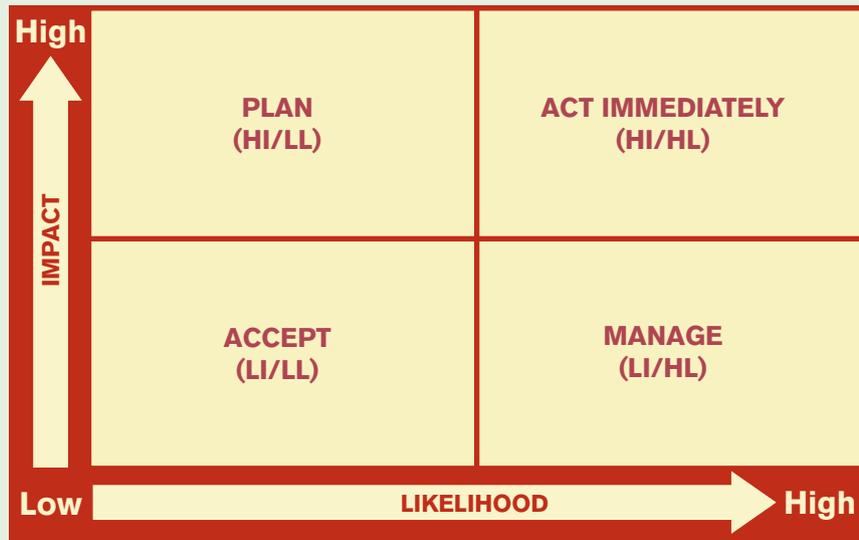
- **risk descriptions:** these should include the sources of the risk, how it might look if it were to impact on the business, and the effect it would have;
- **impacts:** these should be considered in terms of the negative effects on costs, business timetables and overall performance of the business;
- **risk owner:** this should be an individual(s) who is best placed to manage the risk effectively and be responsible and accountable for this task; and
- **action plan:** this is a plan that documents the actions being taken to mitigate both the likelihood of the risk and its impact on the business.

The diagram opposite shows in general terms the types of activity that should be taken into consideration. It is based upon an assessment of the likelihood and impact of the risk.

Assessing risk

Assessments of the likelihood and impact of a risk are by their nature subjective. You can improve your assessment by:

- making use of the best available information about the risks;
- making use of any previous personal or organisational experience and knowledge about the risks;
- being aware of the business's risk appetite in relation to specific risks; and
- identifying your business-critical assets.



PLAN (High Impact/Low Likelihood)

Think about the risk and how you might remove or reduce any negative outcomes. Remember, just because a risk has a low likelihood, that does not mean that it will not happen.

ACCEPT (Low Impact/Low Likelihood)

Accept the risk and do little to control any negative outcomes. Remember, it is very important to have as much information about the risk as possible, if you plan to decide on this option.

ACT IMMEDIATELY (High Impact/High Likelihood)

You must act immediately, treating the risk so that any negative outcomes are removed or severely diminished. What you must aim to do is reduce the likelihood and impact to as low as is reasonably practicable.

MANAGE (Low Impact/High Likelihood)

Manage the risk by putting measures in place to diminish any negative outcomes.

Risk appetite



What does risk appetite mean?

Every organisation and individual will have a level of appetite for risk. Explained simply, risk appetite is the total amount of risk an organisation is prepared to accept, tolerate or be exposed to at any point in time, in the pursuit of its business objectives.

Organisations that are 'risk-ardent' will embrace risk and accept high levels of it, while those that are 'risk-averse' will tolerate only low levels of risk.

The risk appetite of a business is generally culturally determined and often reflects the nature of the business. Agreeing on the correct risk appetite level is important since it allows you to:

- benchmark the level of risk your business is willing to tolerate;
- review your business's risk exposure, which is important in a changing business environment; and
- assess exposure to new risks, while helping you make decisions on managing them.

Remember, the risk appetite of your business should not focus simply on financial considerations; it should also take account of risks to more intangible assets such as your reputation.

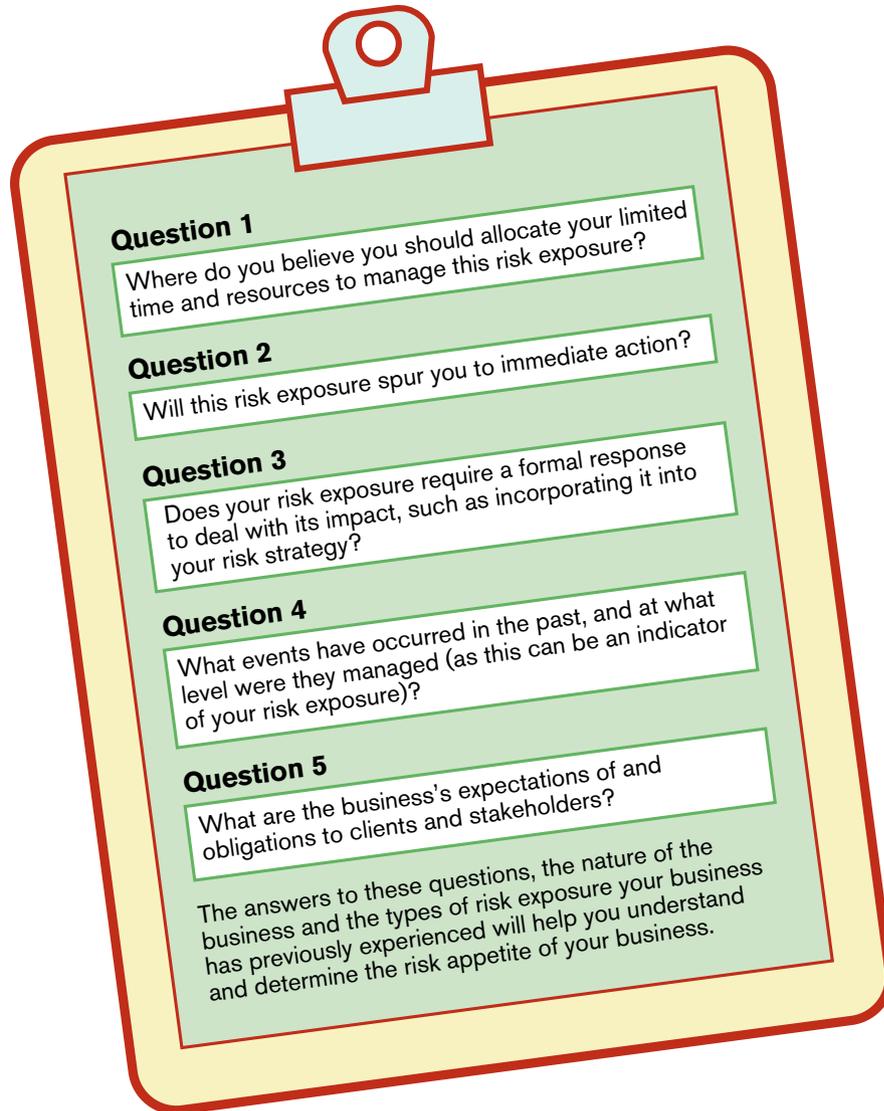
How to determine your risk appetite

As mentioned above, the risk appetite of a business is generally determined by cultural factors.

This is done with the help of the following three factors:

- a desire to carry out normal operations with the minimum of disruption;
- a desire to maximise benefits for the business; and
- a desire to minimise threats to the business.

To help you get a better understanding of risk appetite, consider the following questions about risk exposure. It is advisable to consult widely within your organisation, at all levels, to get the answers you need.



DID YOU KNOW?

Project **Griffin** aims to provide counter-terrorism awareness specifically for security and 'front-facing' staff. Visit the NaCTSO website at www.nactso.gov.uk for more information about Project **Griffin**, and contact your local police and speak with the counter-terrorism security adviser (CTSA) regarding local events.



What action could I take to manage risk?

There are four general approaches to managing risk.

Terminate

Remove the potential impact on the business by stopping the activity at risk or moving from the market/location at risk.

Transfer

Ensure that the consequences of the risk are borne by a third party through insurances or contractual measures.

Tolerate

Accept the potential impact on the business but keep a watch on it.

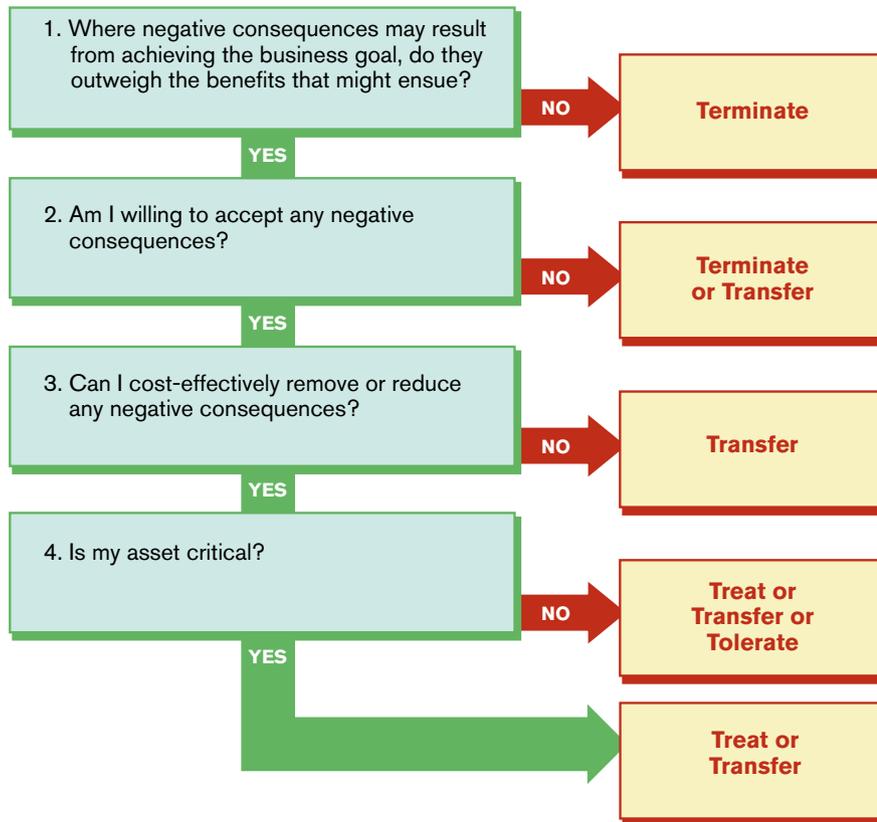
Treat

Apply security or business continuity actions to prevent or mitigate the effects of the risk.

Your action flowchart

Below is an action flowchart that will help you think about the actions you can take in relation to specific risks. It focuses on your business's objectives and assets.

Different risks may require different approaches. These approaches – whether risk management measures or the use of insurance cover – can be blended to meet the needs of the business across different activities and over time.





DID YOU KNOW?

Project ARGUS events are available across the UK and are free. If you take the opportunity to attend one, you will gain a better understanding of the threat from international terrorism and of simple measures that can be taken to protect a business. Visit the NaCTSO website at www.nactso.gov.uk for a list of forthcoming events, or contact your local police and speak with a CTSA.

Risk management and insurance

Calculating the financial costs is just one aspect of managing the risks your business faces. However, there are some financial impacts that you will not be able to calculate easily after a critical event. You will need to manage these and the other risks as carefully as you can.

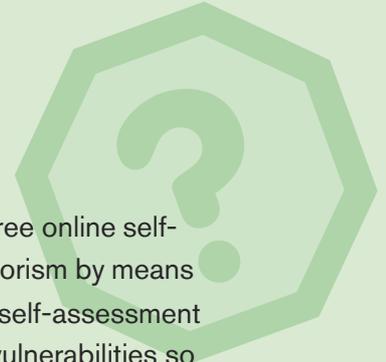
Here are some measures to help you do this.

Put security measures in place to remove or reduce vulnerabilities

Although you cannot remove all security threats to your business, you can remove or reduce your vulnerabilities. You are probably already managing some of your business's vulnerabilities by protecting your products and maintaining your customer base. However, every business needs to think more carefully about the risks from crime and terrorism.

DID YOU KNOW?

Businesses are able to carry out their own free online self-assessment of the threat they face from terrorism by means of an application known as the vulnerability self-assessment tool (VSAT). The tool helps to identify their vulnerabilities so that these can be effectively addressed. Go to the NaCTSO website at **www.nactso.gov.uk**



You will need to identify the threats and hazards to your business, especially those that could have a significant negative impact, such as preventing you from carrying out business activities. You must then identify the business assets that are most likely to be affected by the threats and hazards.

It is useful to draw up a risk register that identifies the critical risks to your business and the key assets affected. When you have identified the risks and assets you will have to assess your appetite for risk.

Transfer some or all of the financial impact of a potential vulnerability

Transferring some of the vulnerability by having insurance in place will ensure some financial recompense if a critical event occurs. However, it cannot replace lost information or repair damage to your business reputation.

It is best to consider insurance for some risks, in conjunction with good security measures for others. You may also be able to transfer some of the risks through contractual arrangements, so that a contractor carries a proportion of the overall risk.

Insurance



What are the benefits of insurance?

There are numerous benefits to insurance, especially in terms of critical events such as terrorism.

Insurance can:

- offer coverage for buildings and contents against physical loss or damage by an act of terrorism. It can also protect against business interruption, whether caused by terrorism, natural disaster (e.g. a flood) or loss of power supply;
- spread the financial losses of an individual undertaking among many policy holders. As a result, no one business need suffer a loss and risk a business failure;
- provide peace of mind for the insured, shareholders, customers and suppliers; and
- help you to focus on investing in your business rather than keeping back unnecessary reserves for emergencies.

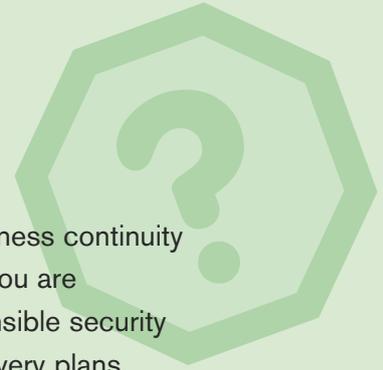
What's the deal on cheap insurance?

Very often it is thought that obtaining short-term premium reductions is good value for money. In certain circumstances this may be true, for instance with car insurance. However, if you are looking at the longer-term health of your business other factors may be more important to you.

Getting insurance at the best possible price is important, but longer-term insurance costs are equally important. Being confident about the cost of your insurance over the next few years allows for better financial planning. Short-term financial savings may appear attractive, but stable insurance costs provide a better financial foundation for managing risks.

DID YOU KNOW?

In order to ensure that your security and business continuity plans remain viable you should behave as if you are uninsured, even if you are insured. Taking sensible security precautions and having tested business recovery plans are essential.



Using insurance to manage risk

Insurance can provide you with a financial safety net in situations where you may not be able to either wholly or partially treat a risk.

When looking at insurance as a risk management option you should:

- do your research: find out which insurance is relevant to you and seek independent advice;
- understand how and when insurance may pay out following a critical event;
- remember that you may incur reinstatement costs quite soon after a critical event; and
- integrate insurance into your risk management plan: consider security and business continuity plans as central to your approach, with insurance in support of them.

Insurance products

There are many insurance products available on the market and it is important that you use products that best meet your needs. You will require some insurance by law, such as employer's liability insurance. Others may be more discretionary, for example personal accident insurance, which comes into play if an accident occurs at work and no fault needs to be proved. The most numerous insurance claims following the 9/11 attacks were of this type.

Terrorism insurance

The Pool Re scheme has been set up by the insurance industry in co-operation with the UK Government so that insurers can continue to cover losses resulting from damage caused by acts of terrorism to commercial property in Great Britain.

The scheme takes two important pieces of information into account when providing insurance cover:

- the financial value of your business properties; and
- the location of these properties.

There are conditions attached to this insurance cover. For instance:

- all your properties have to be insured;
- it does not take account of current risk mitigation measures; and
- no excess is taken into account.

Remember, terrorism cover is normally excluded from ordinary buildings and business interruption insurances, so you will need to buy insurance for that specific risk.

DID YOU KNOW?

If you are a tenant in a building, your commercial lease may well include terrorism cover. Check your conditions and cover – your landlord may be able to help.



Terrorism cover is priced against the value of your buildings, and can never fully financially compensate you for the losses to your business. As a result, you need to ensure that you have adequate security and business continuity plans in place.

Premiums dependent on location

Insurance cover provided under the Pool Re scheme is divided into different zones across the UK. The amount you pay in premiums is partially dependent upon where you are located.

In calculating the cost of cover under this scheme, the value of the property is arrived at and the zones provide a weighting factor that determines the final cost of the cover as a percentage of the property portfolio's value.

You can obtain such cover by contacting your usual insurance broker, who may also be aware of alternative options to Pool Re.

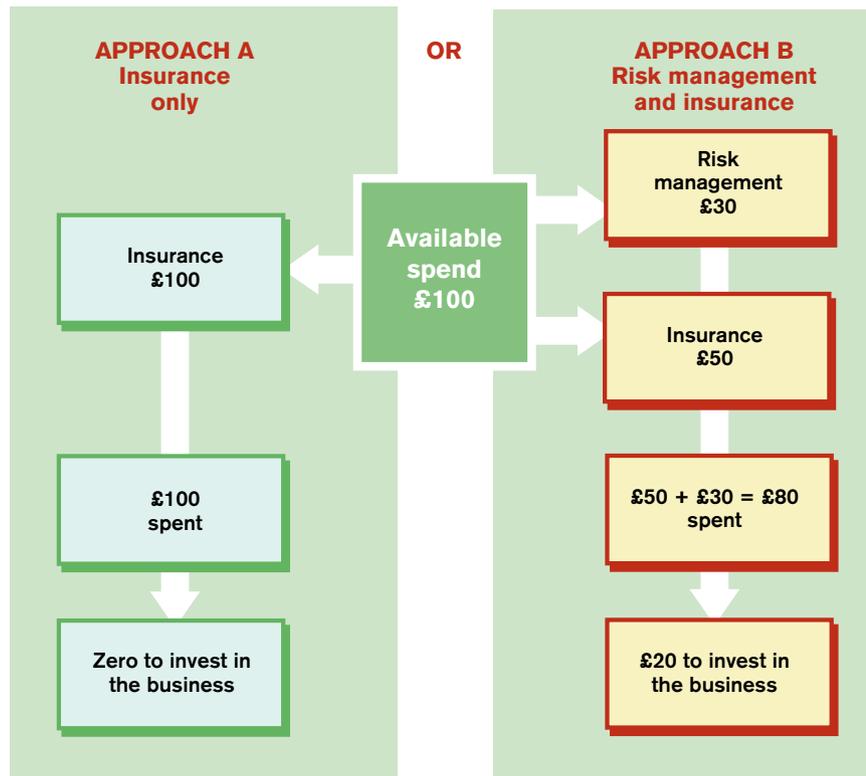
Maximising your protection



Blending approaches for better protection

Taking a risk management approach to protecting the important parts of your business makes sense. When you combine this with the appropriate insurance cover, it not only protects your business but also releases capital that can be used to build your business.

Here is how it works. Imagine taking two approaches to managing risk. Approach A uses only insurance to manage risks. Approach B takes a risk management approach combined with appropriate insurance. As an example, both approaches are given £100 to invest in managing risks – see the diagram below.



Approach B has three advantages over approach A, as follows:

- it helps you to understand your business better;
- it reduces the impact of insurance market volatility; and
- it releases monies that are available to reinvest in the business.

By blending effectively your risk management approach with insurance you can release funds to reinvest in the business, allowing it to grow while at the same time providing the vital protection it needs. So getting your risk management right allows your business to grow.

Tolerating the risk

Doing nothing will leave your business dangerously exposed and it is likely that – sooner rather than later – a vulnerability will be exploited, bringing your business to a halt or seriously disrupting it. Remember, it is not only your people and physical assets that can be adversely affected, but your reputation and the goodwill of the business as well.

As we have seen, there are very good reasons to manage the risks to your business. There may be circumstances where you decide to do nothing about the risk and not take advantage of any of the approaches outlined in this guide. However, there will be very few circumstances where nothing can be done to deal with the risk. If you decide to do nothing, you should regularly review the situation with the presumption that action is better than inaction.

Your checklist



The 10-question checklist

Take a moment to answer these ten questions.

	Y	N
1 Have you identified the threats and hazards to your business?	<input type="checkbox"/>	<input type="checkbox"/>
2 Have you quantified the likelihood and impact of the threats and hazards?	<input type="checkbox"/>	<input type="checkbox"/>
3 Have you identified any risks you cannot influence directly?	<input type="checkbox"/>	<input type="checkbox"/>
4 Have you assessed your appetite for risk?	<input type="checkbox"/>	<input type="checkbox"/>
5 Have you completed the online self-assessment process? ¹	<input type="checkbox"/>	<input type="checkbox"/>
6 Have you identified the assets at risk and actions to be taken?	<input type="checkbox"/>	<input type="checkbox"/>
7 Have you included reinstatement costs in restoring the value of the asset?	<input type="checkbox"/>	<input type="checkbox"/>
8 Have you prepared your risk register?	<input type="checkbox"/>	<input type="checkbox"/>
9 Have you read <i>Expecting the unexpected</i> and <i>Secure in the knowledge</i> ?	<input type="checkbox"/>	<input type="checkbox"/>
10 Have you identified a Project ARGUS or Griffin event to attend?	<input type="checkbox"/>	<input type="checkbox"/>

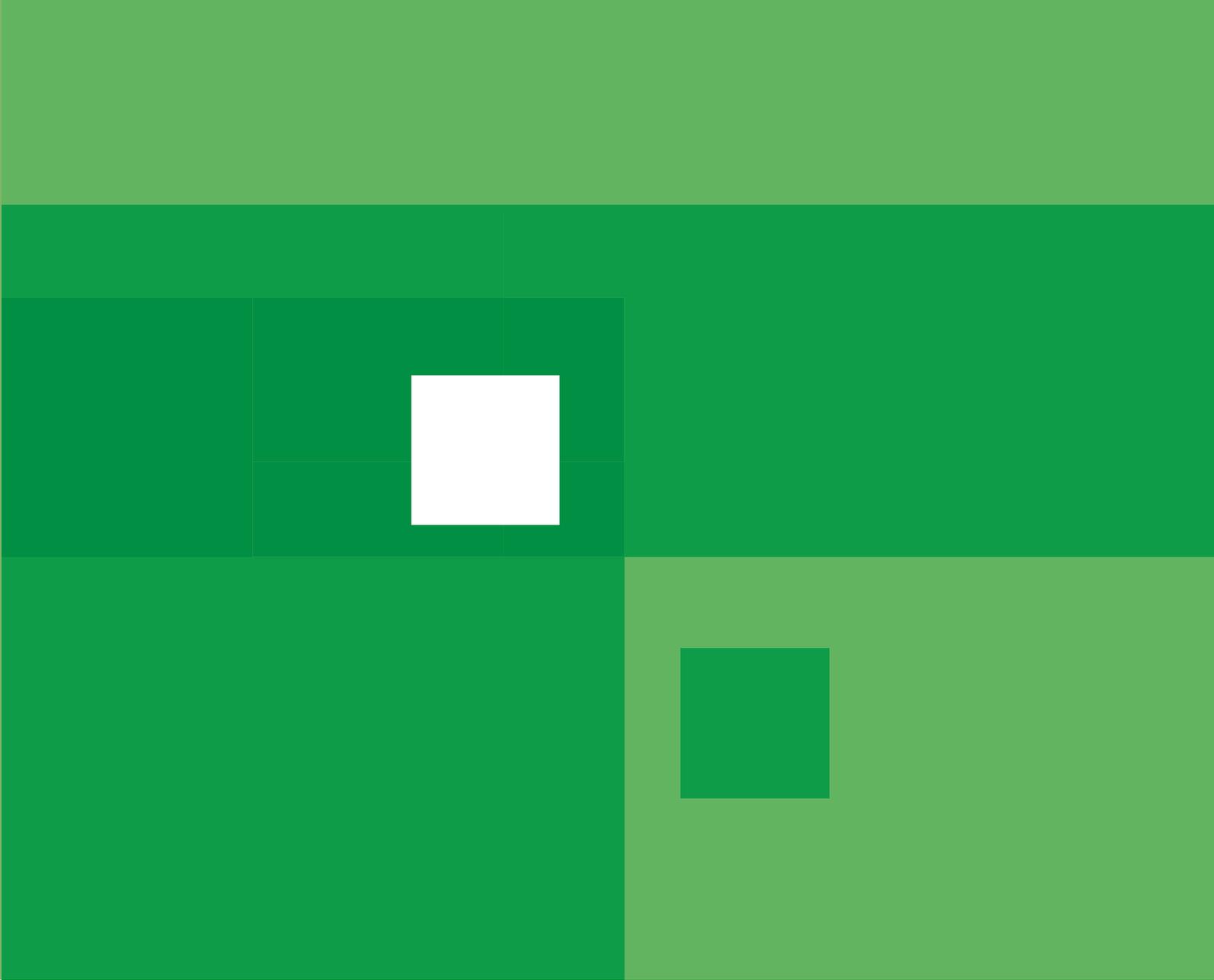
¹ This facility has been temporarily withdrawn (October 2014). Please check the NaCTSO website at www.nactso.gov.uk for updates.

What was your score?

If you answered yes to all these questions, it is highly likely that you have covered all the main areas of work required to improve the security and resilience of your business.

If you answered no to any of these questions, you may need to do further work in this particular area.

It is clear that there is no single solution to dealing with threats and hazards. A flexible, co-ordinated blend of different risk management approaches provides the most cost-effective way to protect your business.



© 2010 London First (Partial Review 2014)

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical or otherwise, without the prior written permission of the publisher.

Produced by the National Counter Terrorism Security Office (NaCTSO)