ProtectUK

Stage 1: Risk Identification

ProtectUK publication date

21/03/2024

The first stage of the risk assessment process is risk identification. This requires you to identify and describe risks that might prevent your organisation from achieving its objectives.



To achieve this, you will be using an **event-based** approach to identifying risk in line with the ProtectUK Approach. This begins with a threat assessment to help you to determine the terrorist threats relevant to your organisation. You will then be guided through a vulnerability assessment to identify the gaps and weaknesses in your current security approach.

Finally, you will be supported in the development a set of **risk scenarios** that capture how a security failure could occur and its potential consequences. This will help to inform your assessment of impact later in the risk assessment process.

As you become more familiar with the risk assessment process, you may wish to adopt an alternative approach to identifying risk. For example, using an asset-based approach instead of an event-based approach. You should consider alternative approaches to identifying risk once you are confident with the process below. Further information on different approaches to risk identification can be found in Section 2 of this guidance.

This stage of the risk assessment process is supported by the ProtectUK Risk Identification Template . The process is broken down step-by-step for you below.

Step 1A: Identifying Threats

The ProtectUK Risk Management recognises 6 key terrorist threats that your organisation may be exposed to:

1. Marauding Attack (MTA)
2. Vehicle as a Weapon (VAW)
3. Improvised Explosive Devices (IEDs)
4. Fire as a Weapon (FAW)
5. Chemical, biological and radiological (CBR)
6. Cyber Attack

To complete the first step of the risk management process, you will need to select which of the above threats you feel your business is exposed to.



This should be recorded in **Part I** of your **Risk Identification Template:**

Attack type	Selected	Rationale	Existing Controls
Marauding attack	☐ Yes ☐ No		
Vehicle as a Weapon	☐ Yes ☐ No		
Fire as Weapon (FAW)	☐ Yes ☐ No		
Improvised Explosive Devices (IEDs)	☐ Yes ☐ No		
Chemical, biological and radiological	☐ Yes ☐ No		
Cyber	☐ Yes ☐ No		

The following questions may help you consider the types of threats that may be relevant to your organisation:

- Are there any types of attack that are common across your industry or sector?
- Are there any types of attack that are common to your location?
- Are there any reasons why you or your neighbouring organisations may be deliberately targeted by an attack?
- Are there any reasons why you or your neighbouring organisations would be easy to attack?
- What work place practices exist which may protect you from, or expose you to, particular attack types?
- Is there anything at your site which could be used to aid an attack (such as fuel stores or chemicals)?

You may find it helpful to look back at previous terrorist attack records or review the Threat Analysis

resources available on ProtectUK when considering relevant threats. These resources may help you identify threats that are less obvious to you. Equally, you may find it useful to consult with the management team and staff within your organisation. These individuals may be able to provide you with further insight around the threats your organisation is exposed. Security specialists and experts and local and national bodies may also be able to provide you with further support during this step.

If you do not consider a particular threat to be relevant to your organisation, you may choose not to take this forward as part of your risk assessment.

Your selected threats and rationale for inclusion and exclusion should be recorded clearly in your template:



Your output at this stage should be: a list of relevant threat types.

Step 1B: Identifying Existing Controls

With the relevant threats to your organisation established, you should now turn your consideration to the control measures you have in place to manage these risks.

When completing this step, you should think about the control measures currently in place across your organisation and whether these are actively contributing to managing terrorist risk.

You may not have introduced any controls with terrorism in mind specifically. However, there may be controls that you have introduced in another risk context that are also working to reduce terrorist related risk. For example, security related controls, such as CCTV, fire safety related controls, or health and safety controls.

It is important that this activity is undertaken as early as possible as this will help to prevent any existing controls from being duplicated as part of your risk treatment efforts later in the RMP.

The controls you identify may be physical controls or active controls:

- **Physical controls** relate to building and infrastructure, equipment and technology. This may include bollards and fences, metal detectors, electronic access controls, alarm systems and CCTV.

- **Active controls** are procedural and concerned with what people do on site and how they do it. This may include procedures relating to visitors, recruitment procedures, training and

exercising, incident response and suspicious items procedures.

For further examples of physical and active controls, see the **ProtectUK Control List.**

Any existing controls you have in place should be briefly listed in your template. You do not need to identify controls for threat types you have deemed irrelevant to your organisation:



Your output at this stage should be: a list of relevant threat types, with rationale for inclusion or exclusion, and a list of any existing controls in place to help manage risk.

Step 1C: Identifying Vulnerabilities

Following the identification of threats and existing controls, you are now in a position to consider the vulnerabilities that may exist in your current security approach. These should be recorded in **Part II** of your **Risk Identification Template**:



Vulnerabilities are weaknesses that may be exploited by a threat to achieve an impact, such as harm to people or your organisation. Vulnerabilities cannot cause an impact in isolation. The presence of a threat is required to exploit a vulnerability to achieve impact.

Vulnerabilities may arise from areas where controls are not in place to manage risk. They may also arise from areas where controls have been implemented but are ineffective or malfunctioning.

Ineffective or Malfunctioning Controls

In the previous step, you identified the existing control measures you have in place to help manage the risk posed by terrorist threats. You will now need to confirm that these control measures are working effectively to control risk.

If a control measure is found to no longer be effective, or does not function as expected, this should be considered a vulnerability as this weaknesses may able to be exploited by a terrorist threat to cause harm.

To determine whether there is an issue with a control you have in place, you will need to undertake a systematic review. This requires you to observe the environment in which the control has been implemented and review the design of the control itself to look for potential weaknesses. You should also look to review any documentation of the control operating in practice and the performance of the control if this is available i.e. the reduction in risk and incidents that has occurred following

implementation.

Different individuals within your organisation may be able to assist you with confirming the effectiveness of a control. For example, a CCTV Operator or Security Manager may be able to provide you with information or review documentation regarding the functionality and effectiveness of a CCTV system and other security equipment. You may also wish to consult with subject matter experts.

If you identify a control measure that is no longer working effectively, such as malfunctioning CCTV or broken perimeter fencing, this should be noted as a vulnerability in your template.

Missing Controls

Vulnerabilities may also arise where you have no control measures in place to help manage risk. This may include the absence of controls across areas such as:

- **Policy and Procedure**

Security policies and procedures provide management direction and support in accordance with business requirements and relevant laws and legislation. A failure to determine appropriate security policies and procedures may result in greater harm to your organisation due to a lack of leadership and control in response to security incidents.

- **Organisational Arrangements**

Internal and external arrangements are essential to ensure the effectiveness of your security approach. These arrangements should be regularly reviewed and clearly communicated across your business. The absence of such a framework may leave your organisation vulnerable to attack as key roles and responsibilities may not be outlined or allocated and external arrangements with neighbouring businesses and partners may not be established or adequately maintained.

- **People and Personnel**

Employees and contractors should clearly understand their roles and responsibilities in relation to security and counter- terrorism. These individuals must be suitable for the roles for which they are considered. A failure to properly verify the suitability of employees or provide adequate training may increase the likelihood of a successful attack by limiting awareness and exposing your organisation to insider threats.

- **Access Control**

Failures in access control could increase the likelihood of a successful attack by enabling unauthorised persons access your organisation and assets. This may be achieved through a lack of robust visitor procedures or poor review of user access rights, particularly when staff leave your organisation.

- **Physical Environment**

Protection of your physical environment enables you to prevent the occurrence of unauthorised physical access, damage and interference to you organisation. A failure to secure offices, rooms, facilities and perimeters may enable unauthorised individuals access to your site and / or equipment, increasing the likelihood of a successful attack.

- **Cyber Security**

Cyber security ensures the protection and security of information generated, stored or transferred by your organisation. Failure to account for cyber security increases the likelihood of a cyber-attack, which may result in denial of service or theft of sensitive and personal information. The likelihood of a cyber-attack may be increased as a result of poor password management systems and a lack of controls against malware.

- **Asset Security**

Failure to account and adequately protect key organisational assets, such a technology and equipment, may increase the likelihood of their exploitation by a terrorist threat. This could arise following the unauthorised removal of assets off-site or due to a failure to provide adequate security for assets off-premises.

- **Service Delivery**

Adequate service delivery and house-keeping reduces opportunities for interference across your organisation. This also helps to reduce and manage the occurrence of false alarms and hoaxes. If your organisation does not have the assurance of robust house-keeping procedures, the likelihood of a terrorist threat being able to exploit these weaknesses increases. For example, poor waste disposal management may increase the likelihood of an IED remaining undetected. Inadequate estates management may result in CCTV being obstructed by overgrown trees and bushes, decreasing your ability to detect potential threats entering or exiting your site.

- **Communications**

Inadequate internal and external communications may be easily exploited by terrorist threats to increase the likelihood of a successful attack on your organisation. This may arise from a failure to adopt a security-minded communications strategy, resulting in sensitive information being publicly available to hostile actors on websites and social media that can then be exploited to gain unauthorised access to your site, or from a lack of established communications with neighbouring businesses, support networks and law enforcement agencies, resulting in a lack of preparedness in the event of an attack.

- **Security Incident Preparedness and Response**

Security preparedness and response plans ensure that your organisation has made adequate preparations to effectively respond to a security incident. Without these preparations, you will not be able to respond to a terrorist attack effectively. This could increase the likelihood of an attack being successful with high impact. Failures in security incident management include a lack of a reporting procedure for security incidents and suspicious items, the absence of set plans and procedures for different attack types e.g. bomb threats and marauding terrorist attacks, or a lack of available resources in response to security incidents e.g. first aid equipment.

- **Security Incident Management**

Security incident management helps to ensure a consistent and effective approach to the management of security incidents. These types of failures may follow from a lack of an Incident Management Plan (IMP), or from poor evidence collection procedures post-incident, preventing the improvement of future security arrangements.

- **Business Continuity**

Planning and making business continuity arrangement will enable you to maintain critical and urgent business activities in the event of a terrorist incident. Failure to make suitable arrangements and embed procedures to ensure an adequate level of service may increase the impact of an attack on your organisation. This could result in substantial financial losses and extensive or permanent disruption to service.

The examples provided above are not exhaustive. There may be other areas of vulnerability that exist across your organisation that are not listed here, or new vulnerabilities that emerge across different areas through time. Identifying vulnerabilities should therefore be an ongoing activity in your

organisation, rather than a one-off exercise.

You should revisit this step of the risk assessment process periodically, particularly when there has been a change to your organisation, or a change in the threat landscape. These changes can lead to the emergence of gaps and weaknesses that your assessment has not yet accounted for.

You may find it helpful to conduct a walkthrough of your organisation in order to help identify vulnerabilities. This may include speaking to management and staff to help you identify gaps and weaknesses in your current security approach or consulting with security specialists and experts.

If this is the first time you have undertaken a vulnerability assessment from a counter-terrorism perspective, you may also find it useful to review the **ProtectUK Control List** as part of this step. The ProtectUK Controls List provides a comprehensive list of controls that can be implemented by a business to manage terrorist risk.

Example Controls from ProtectUK Controls List:



The absence of controls in your organisation against those listed in the ProtectUK Controls List may help you spot gaps and weaknesses in your current approach. These gaps could be considered vulnerabilities.

For example, **Control A.3.** refers to the review of security preparedness and response policies. If you do not review your security policies regularly, they may quickly become outdated and ineffective. This could result in key roles and responsibilities being allocated to retired posts, points of contact and references being outdated, or new attack types being unaccounted for. This may cause severe harm to your employees and the general public if not addressed as you would ultimately lack the planning and direction required to mitigate the consequences of an attack. As such, the absence of Control A.3. suggests a gap in your security approach that should be recorded in your template as a vulnerability.

Each vulnerability you identify should be briefly summarised in your template:



Your output at this stage should be: a list of vulnerabilities identified across your organisation.

Step 1D: Identifying Consequences

You are now in a position to consider the consequences that would follow from each vulnerability

being exploited by a relevant threat type. This is achieved through the development of **risk scenarios**.

A risk scenario essentially describes a security failure by bringing together a threat, event and consequence in a narrative description. These scenarios help you to explore what could go wrong in your organisation and how.

Working through risk scenarios is an important step in the risk management process as this will help you to determine the loss or harm that may be caused by security failure.

In order to construct a risk scenario you will need to address the following questions:

- **Threat**: who is capable of exploiting the vulnerability?
- **Event**: what could go wrong and how this could happen?
- **Consequence**: what harm or loss could be caused?

Part II of your **Risk Identification Template** has been designed to support you in building these scenarios step-by-step:

Threat

Your risk scenario begins with identifying the threats capable of exploiting the vulnerability you have identified.

For each vulnerability, you should consider whether the weaknesses or gap you have recognised could be exploited by:

- **A single threat source**

The vulnerability is capable of being exploited by one threat, such as a cyber-threat

- **Multiple threat sources**

The vulnerability is capable of being exploited by more than one threat, but not all threats. For example, a cyber-attacker and an marauding attacker

- **All threats**

The vulnerability is capable of being exploited by all identified threats

It is entirely possible that some of the vulnerabilities you identify could be exploited by all threat types as opposed to a single threat or multiple threats. For example, if you lack a security policy in your organisation, this could be indicative of an overall lack of strategic direction in response to security incidents. This could be exploited by all threat types to cause harm. Where you find this to be true for a vulnerability, you should record ‘all threats’ in the ‘threats’ column in your template.

For single threats, note the specific threat type in the ‘Threat’ column.

For multiple threats, you will need to duplicate the vulnerability identified in your template and list each applicable threat individually. This will enable you to construct a more specific risk scenario than if you were to group these threats together.

Vulnerability	Threat	Event	Consequences
There are currently no review procedures in place for security related procedures	All threats		
Passwords used on staff accounts for laptops / desktops do not require strong passwords	Cyber-attack		
Local suppliers used for food and drink are unable to offer reassurance regarding food and drink defence	CBR attack		

Event

You should now look to describe the circumstances in which the threat(s) you have identified could exploit each vulnerability. This means describing what could go wrong and how this could happen.

Your description should present a brief narrative of how a security incident may unfold. This could include the methods that a threat might employ to cause harm, such as contaminating products, infecting malware systems, or concealing and detonating an IED.

You should record your description of each event should be recorded in your template under the ‘Event’ heading.



Consequences

In order to complete your risk scenario, you will need to establish the consequences that could follow each event. This concerns the loss or harm that might be caused to your organisation or to staff, customers and others.

The following questions can help you to work through the potential outcomes of each particular scenario:

- Who might be harmed and how?
- What other consequences might there be?
- Will the consequences be short term or long term?

The consequences of an attack may be felt by your organisation immediately. This could include loss of life or structural damage to your site. Other consequences may be experienced by your organisation through time. For example, loss of staff contributing to resourcing issues that impact the achievement of your objectives.

As you consider each event, you will need to think through the possible outcomes and consequences this could cause across your organisation. This may include consequences across the following areas:



- **Life and Safety**

Consequences that concern life and safety are often highly visible outside of your organisation. They include minor – severe injuries, stress and trauma, and loss of life. A terrorist attack may also have an adverse effect on your employees by contributing to low staff morale and resourcing issues. This may produce secondary operational and financial impacts.

- **Financial**

Financial consequences may be experienced by your organisation immediately post-incident or in the months or years that follow an incident. This may arise from a loss of sales and business opportunities, increased insurance premiums, replacement and redevelopment costs, or contractual penalties.

- **Organisational**

Organisational consequences impede the delivery of key business objectives or projects in your organisation. This can have an indirect operational or financial impact if third parties or service contracts / agreements are involved. Organisational consequences may result in reductions to the scope and quality of projects, delays to project and objective schedules, significant project overrun, or the inability to successfully deliver objectives and projects.

- **Operational**

Operational consequences can impair your business as usual activities. This can often have an indirect financial or organisational impact by forcing you to cease trading and services. This type of consequence may follow from loss or damage to premises and equipment or productivity losses.

- **Environmental**

Environmental consequences concern the adverse ecological effects that could occur following a terrorist attack. This could follow from the discharge of harmful substances to surface or groundwater, or the release of bio-aerosol and pollutants. Environmental consequences are likely to have a secondary impact on life and safety by threatening waterways and agriculture.

- **Legal and regulatory**

Legal and regulatory consequences can have significant repercussion for your organisation. Oftentimes, these are financial and will follow from penalties from sector regulators, fines for malpractice or non-compliance, breach of contract damages, or fraud and other criminal acts. If a terrorist attack impairs your ability to comply with your legislative and statutory duties, you are likely to experience these types of consequences alongside secondary financial and operational impacts as your ability to trade may be negatively affected.

- **Reputational**

Reputational consequences concern your organisation's image and standing. This type of consequence can cause severe harm to your organisation by negatively affecting public and customer perception, industry and institutional image and stock market confidence. This may cause you to lose business to competitors or cease trading entirely if you experience a total loss of confidence.

As you work through each scenario, you should ask yourself whether any potential harm or damage could arise across each of these categories. Any consequences you identify should be briefly described in your template under the 'Consequences' heading:

Vulnerability	Threat	Event	Consequences
There are currently no review procedures in place for security related procedures	All threats	Attacker employs new methods to launch a successful attack as current policies and procedures are not updated regularly	• Loss of life • Loss of public confidence which will impact profits
Passwords used on staff accounts for laptops / desktops do not require strong passwords	Cyber-attack	Cyber threat obtains sensitive customer information via password attack as no password management is currently in place	• Breach of legislative requirements which could lead to investigation • Loss of public confidence
Local suppliers used for food and drink are unable to offer reassurance regarding food and drink defence	CBR attack	CBR threat compromises food supply chain to contaminate products served to the public / staff as there no procedures in place to detect tampering	• Loss of life • Loss of public confidence which will impact profits

Note: the consequences above are not exhaustive. There may be other types of consequences that are relevant to the scenarios you are exploring. You should include any consequence that you feel is relevant to your organisation and the scenario you have developed.

This completes the risk identification stage of the RMP. You have successfully developed a list of risk scenarios. These scenarios will now be taken forward into the next stage of the process: Assess the Risks.

Your output at this stage should be: a list of vulnerabilities, relevant threat types, events and consequences (risk scenarios)

KEYWORDS

RISK MANAGEMENT
RISK ASSESSMENT
RISK
RESPONSE
PROTECTIVE SECURITY

PAGE CATEGORY

SECURITY RISK MANAGEMENT