ProtectUK

Risk Management Process

ProtectUK publication date
19/03/2024

Why do you need to manage your security risks?

While it’s true you’re very unlikely to be caught up in a terrorist attack, as an employer, you are required by law to protect employees, customers, volunteers and other people visiting your sites from harm.

If you’re unfortunate enough to be part of an attack, you need to have a system in place to identify and manage the risks. This will help your organisation to keep people safe and give confidence to those working in or visiting your site by showing that you have taken measures to protect them. This will also reduce the adverse effects that might result from an attack, helping you to protect your reputation or brand and minimise financial losses.

This guidance provides information which will help you take forward a strong risk management system which will prepare your organisation to cope better if you should be caught up in an attack.

The following sections provide a broad overview of the ProtectUK approach and its supporting resources.

The ‘related content’ page on ProtectUK’s Risk Assessment process will take you through this approach step-by-step.

ProtectUK Risk Management Process

The ProtectUK Risk Management Process (RMP) has been tailored specifically to manage terrorist risk. It is adapted from the general risk management process found in a number of standards, including ISO/IEC 31000 and ISO/IEC 27005. The approach consists of five key stages that capture the following core ProtectUK risk assessment activities:

- **Stage 1:** Identify the risks (risk identification)
- **Stage 2:** Assess the risks (risk analysis and evaluation)
- **Stage 3:** Treat the risks (risk treatment)
- **Stage 4:** Record your actions
- **Stage 5:** Review

The above activities are supported by the ProtectUK risk assessment templates:

- **ProtectUK risk identification template**
  Supports stage 1 of the ProtectUK risk assessment process
- **ProtectUK risk assessment template**
  Supports stages 2-3 of the ProtectUK risk assessment process

The process of recording and reviewing (stages 4-5) are actively supported by the consistent use of these templates.

The ‘related content’ page on ProtectUK’s Risk Assessment process will take you through this approach step-by-step.

ProtectUK Approach

The **ProtectUK approach** identifies risk by considering relevant terrorist threats and examining risk scenarios. A qualitative risk analysis methodology, generic risk criteria, and a risk matrix are utilised to assess and evaluate risk. The methods and techniques that make up the ProtectUK approach are discussed in greater detail throughout this guidance.

While the ProtectUK approach forms the basis of this guidance and is freely available for use, its primary intention is to act as a broad example. This is due to its generic nature. In order for you to gain the most value and insight from the risk management process, your risk assessment should move beyond the generic to capture your organisational context and risk appetite. To support you in achieving this, the ProtectUK approach is presented alongside additional information and guidance that will help you tailor your approach to your organisational needs.

ProtectUK Controls List

In risk management, a control is any measure or action that modifies risk. In order to address the risk of terrorism, you will need to introduce controls that modify the risk you face to an acceptable level for

your organisation.

The ProtectUK Controls List has been designed specifically to help you achieve this. The list takes its inspiration from the operational level controls included in ISO/IEC 27001, and groups a number of broad controls across 12 distinct categories:

1. Policies and Procedures
2. Internal Organisation
3. People and Personnel
4. Access Control
5. Physical Environment Security
6. Cybersecurity
7. Asset Security
8. Service Delivery
9. Communications
10. Security Incident Preparedness and Response
11. Security Incident Management
12. Business Continuity

The ProtectUK Controls list may be used in conjunction with the enhanced controls captured within the Menu of Tactical Options (MoTO) to help manage terrorist risk.

Menu of Tactical Options (MoTO)

The Menu of Tactical Options provides a list of prescriptive, enhanced controls that should be considered to support your business when there has been an increase in threat level to critical, or following an incident or attack. These controls may be introduced alongside the controls listed in the ProtectUK Controls List to offer an enhanced response to potential terrorist threats. This may include stepping up the measures you already have in place, or introducing new controls temporarily.

The control measures outlined in MOTO are intended for implementation during times of increased risk and may be unsuitable or unsustainable for your organisation in the long-term. This is due to the increase in resource and financial commitment that these controls are likely to require. MOTO controls should therefore be subject to informed revision when the threat level decreases. This should be assessed and evaluated using the RMP.

KEYWORDS

RISK MANAGEMENT
RISK ASSESSMENT
RISK
RESPONSE
PROTECTIVE SECURITY

PAGE CATEGORY

SECURITY RISK MANAGEMENT