ProtectUK

Risk Management Guidance

ProtectUK publication date

19/03/2024

Risk management can assist you with making effective and timely decisions across your organisation. This can help to increase the likelihood of you achieving your objectives and ensuring public safety, even if you are caught up in a terrorist attack.

Introduction

The following guidance will help you to plan and implement an effective programme of terrorist risk management in your organisation. This is delivered across three core sections:



1. Setting the Scene

This section introduces some of the key elements you need to establish before undertaking a terrorist risk assessment. This includes setting the scene for your risk assessment, establishing governance

arrangements, and the setting of your organisational risk appetite.

2. Risk Management Basics
This section introduces the core components of a risk assessment, including common risk assessment approaches and techniques. Key considerations for adapting your approach to assessing risk are also presented here.

3. Risk Assessment Process
This section provides a step-by-step breakdown of the ProtectUK Approach to assessing risk, including risk identification, risk analysis and evaluation, and risk treatment. These activities are broken down across 5 distinct stages with supporting resources signposted where relevant.

It is highly recommended that you review all sections of this guidance before undertaking your risk assessment.

How to use this guidance

This guidance has been produced primarily for those undertaking a risk assessment for the first time. Its aim is to provide a comprehensive understanding of core risk management concepts and approaches to support new assessors in completing an effective risk assessment.

To gain the most value from this guidance, you should move through each of the above sections in the order they are presented above:

1. Setting the Scene
2. Risk Management Basics
3. Risk Assessment Process

Section 1 and 2 of this guidance – Setting the Scene and Risk Management Basics – will provide you with the core knowledge required to undertake an effective risk assessment. These sections will help you understand core concepts, how to plan for a risk assessment, and how to tailor a risk assessment to suit your organisational needs and context.

Section 3 of this guidance – Risk Assessment Process – then presents a step-by-step breakdown of how to undertake a risk assessment. This guidance follows the ProtectUK Approach to assessing risk and is supported by the use of the ProtectUK Templates.

The ProtectUK Approach is a pre-set, generic approach to assessing terrorist risk. It is intended to help build your maturity and confidence with managing risk.

Once you are comfortable with how to undertake a risk assessment, you should return to Section 1

and 2 of guidance to consider how you might tailor your risk assessment to better suit your organisation needs and context. You will find further information on how to customise and adapt your risk assessment throughout this guidance.

Key Terms

risk
effect of uncertainty on objectives

risk scenario
sequence or combination of events leading from the initial cause to the unwanted consequence

risk owner
person or entity with the accountability and authority to manage a risk

risk source
element which alone or in combination has the potential to give rise to risk

risk criteria
terms of reference against which the significance of a risk is evaluated

risk appetite
amount and type of risk that an organisation is willing to pursue or retain

threat
potential cause of a security incident that can result in damage to a system or harm to an organisation

vulnerability
weakness of an asset or control that can be exploited so that an event with a negative consequence occurs

event
occurrence or change of a particular set of circumstances

likelihood
chance of something happening

consequence
outcome of an event affecting objectives

level of risk
significance of a risk, expressed in terms of the combination of consequences and their likelihood

control
measure that maintains and/or modifies risk

residual risk
risk remaining after risk treatment

risk management process
systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk

risk assessment
overall process of risk identification, risk analysis and risk evaluation

risk identification
process of finding, recognising and describing risks

risk analysis
process to comprehend the nature of risk and to determine the level of risk

risk evaluation
process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its significance is acceptable or tolerable

risk treatment
process to modify risk

risk acceptance
informed decision to take a particular risk

risk sharing
form of risk treatment involving the agreed distribution of risk with other parties

risk retention
temporary acceptance of the potential benefit of gain, or burden of loss, from a particular risk

Source: ISO Guide 73:2009; ISO 31000:2018; ISO 27005:2022

Further reading

- ISO/IEC 31000 – Risk Management
- ISO/IEC 27005 – Information Security, Cybersecurity and Privacy Protection – Guidance on Managing Information Security Risks
- NPSA – Protective Security Risk Management (PSRM)
- NCSC – Risk Management Collection

KEYWORDS

RISK MANAGEMENT
RISK ASSESSMENT
RISK
RESPONSE
PROTECTIVE SECURITY

PAGE CATEGORY

SECURITY RISK MANAGEMENT