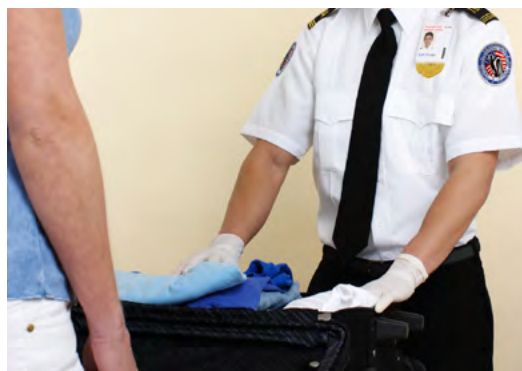


PAS 127:2014

Checkpoint security screening of people and their belongings – Guide



Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2014. Published by BSI Standards Limited 2014

ISBN 978 0 580 79006 5

ICS 13.310

No copying without BSI permission except as permitted by copyright law.

Publication history

First published February 2014

Contents

Foreword	iii
Introduction	iv
1 Scope	1
2 Terms, definitions and abbreviations	2
2.1 Terms and definitions	2
2.2 Abbreviations	4
3 Outline of process	5
4 Assessing the risk	7
4.1 General	7
4.2 Risk assessment process	7
4.3 Recording and presenting the results	8
4.4 Risk management and mitigation	9
4.5 Risk assessment review	9
5 Checkpoint screening requirements	10
5.1 General	10
5.2 People flows, throughput and belongings	11
5.3 Temporary checkpoints	11
5.4 Location of screening facilities	11
5.5 Associated security measures	12
5.6 Checkpoint layout	13
5.7 Recording the operational requirements	13
6 Screening strategies	14
6.1 General	14
6.2 Implementation	14
6.3 Managing fluctuations in demand	15
6.4 Future proofing	15
7 Technologies and methods	16
7.1 General	17
7.2 Screening technologies and methods	18
7.3 Combining detection technologies and methods	24
8 Implementation and deployment	26
8.1 General	26
8.2 General physical security measures	26
8.3 Management and responsibility	26
8.4 Operating procedures	26
8.5 Checkpoint design considerations	28
8.6 Equipment ownership considerations	29
8.7 Screening staff considerations	30
8.8 Health and safety	32
8.9 Security procedures	32
8.10 Authority and consent to screening	33
8.11 Privacy and ethical issues	33



9 Monitor effectiveness and review	34
9.1 General	34
9.2 Performance measures	34
9.3 Continuous performance monitoring	35
9.4 Periodic performance testing	35

Annexes

Annex A (informative) Location of screening facilities	36
Annex B (informative) Relevant standards	38
Annex C (informative) Action upon discovery of a threat item (or a suspicious item that could be a threat item)	42

Bibliography	43
Standards publications	43
Other publications	43
Further reading	43
Websites	43

List of figures

Figure 1 – Summary of PAS 127 process	6
Figure 2 – Plot of impact of a threat scenario versus its likelihood	9

List of tables

Table 1 – Common security screening methods and technologies	16
Table 2 – Common approaches to combining person search and search of bags/possessions, with example applications	25

Foreword

This PAS was sponsored by the Home Office Centre for Applied Science and Technology (CAST). Its development was facilitated by BSI Standards Limited and published under licence from The British Standards Institution. It came into effect on 28 February 2014.

BSI wishes to acknowledge the following organizations that were involved in the development of this PAS as members of the steering group:

- Airlock Aviation
- BAA
- Centre for the Protection of National Infrastructure
- Defence Science and Technology Laboratory
- Department for Transport
- Glasgow 2014 Ltd
- Home Office
- Iconal Technology Ltd
- Metropolitan Police Service
- Security Industry Authority
- Security Institute
- Sodexo

Wider comments from other interested parties were invited by BSI. The expert contributions made by the organizations and individuals consulted in the development of this PAS are gratefully acknowledged.

The British Standards Institution retains ownership and copyright of this PAS. BSI Standards Limited as the publisher of the PAS reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in *Update Standards*.

The PAS process enables a specification to be developed rapidly in order to fulfil an immediate need in industry. A PAS may be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The provisions of this PAS are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”. The use of the auxiliary verb “can” indicates that something is technically possible and the auxiliary verb “may” indicates permission.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Spelling conforms to *The Shorter Oxford English Dictionary*. If a word has more than one spelling, the first spelling is used.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with this PAS does not itself confer immunity from legal obligations.

This document has been prepared for guidance only. Whilst considerable care has been taken in preparing the information contained within it, no responsibility or liability is accepted for any injury, loss or damage incurred as a result of any use or reliance upon the same. Adherence to the guidance does not ensure compliance with relevant legal obligations. If in doubt users should take appropriate advice. The guidance is a living document and may be revised periodically as necessary.

Introduction

An unfortunate feature of modern society is that buildings, sites, sporting and other public events may be targets for terrorist or other malicious attacks. It is necessary to remain vigilant to prevent such attacks as well as to protect people and infrastructure from their effects.

This PAS is the first publication of its kind to present guidance on good practice for checkpoint security screening of people and their belongings in buildings and at large events. It has been developed using information derived from a wide range of security experts in industry, government, academia and law enforcement agencies.

Insufficient or inappropriate security measures may be ineffective at reducing the risk of adverse incidents and in some cases may even increase this risk. Conversely, excessive measures will result in unnecessary expense and use of staff and space, and are likely to interfere with the normal functioning of the site or event being protected.

This PAS addresses the scarcity of information on checkpoint security screening in non-regulated environments. It aims to give guidance on good practice for setting up checkpoint security systems in public spaces, government and other sensitive buildings, secure sites, large sporting and other public events. A complete process is outlined, from assessing the risk, establishing security requirements and selecting screening strategies through to the deployment of suitable methods and equipment. Although the main focus is on permanent checkpoints, the same underlying principles apply to the installation of temporary checkpoints, for example, at large public events. This specification should be useful to all those responsible for designing and delivering security systems and procedures for checkpoint screening. It will also be of interest to equipment manufacturers, procurement managers, policy makers and the Government.

Security is a complex issue. Security screening may be regarded as a system, the function of which is dependent on its components, the interactions between them and the environment. Therefore a systems approach has been used in this PAS. It considers people, processes, information and technologies.



1 Scope

This PAS gives guidance and recommendations for checkpoint security screening of people, and their bags and possessions, for non-regulated applications. This includes both permanent and temporary installations at government and private buildings, events and sporting venues in public spaces or on private land. The PAS focuses on the detection of weapons and explosive threat items but the methodology can equally be applied to address other threats that an organization may face.

This PAS is primarily aimed at anyone who has responsibility for planning and/or delivering security operations at venues in either the private or public sector. It will also be of interest to equipment manufacturers, procurement managers and policy makers. This document provides a framework for assessing risk and identifying screening requirements, and then specifying and delivering appropriate solutions. Key benefits and limitations of common screening methods and technologies are also summarized. The PAS has been deliberately kept flexible; users may tailor the recommendations to suit the particular requirements of their own organization or event, whilst still adhering to the principles of good practice.

Security checkpoints rarely operate in isolation; recommendations for checkpoint screening are presented in the wider context of the organization's security systems as a whole. These systems may, for example, include physical security measures such as closed-circuit TV surveillance (CCTV), and access control and personnel security, which may include accreditation of staff and visitors.

Security staff form an integral part of any security system. Staff responsibilities are considered at all levels, from senior managers responsible for security or the commissioning of security services, through to the staff who carry out screening of individuals and bags or possessions. The importance of effective and relevant training of staff, maintaining staff motivation and ongoing monitoring of performance is also discussed.

Aviation and other transport security screening are outside the scope of the PAS since these are subject to separate national and international regulation. However, it is important to note that nothing in the current PAS conflicts with well-established aviation security screening procedures. Rather this document seeks to build on the best practices of aviation and other regulated transport

security and to apply these to the non-regulated environment where appropriate. Where gaps have been identified new guidance is provided.

Whilst the prime focus of the PAS is screening for explosives and weapons, the screening procedures described can be adapted to detect or mitigate other types of threat such as:

- a) chemical, biological, radiological, nuclear (CBRN) materials;
- b) other illicit substances, such as narcotics;
- c) other items or materials that the organization might wish to prohibit on safety or security grounds, such as alcohol or medicines;
- d) items that may cause inconvenience or nuisance (such as musical instruments);
- e) theft of physical assets;
- f) industrial espionage;
- g) public disorder or criminal activity.

This PAS does not cover:

- a) vehicle screening;
- b) mail screening (this is covered in PAS 97:2012, *A specification for mail screening and security*);
- c) defensive search of buildings or sites.

NOTE Although specific CBRN screening technologies and methods are beyond the scope of this PAS, measures associated with screening for explosives and weapons can also reduce the risk of CBRN threat items. If, following risk assessment, CBRN threat items are considered likely, expert advice should be sought.



2 Terms, definitions and abbreviations

For the purposes of this PAS, the following terms and definitions apply.

NOTE BS EN 15602:2008, Security service providers – Terminology uses terms and definitions that may have differing meanings to those below.

2.1 Terms and definitions

2.1.1 assurance

level of confidence or degree of certainty that a security screening system can detect and respond to a threat item, and thereby help prevent an attack

2.1.2 authorized personnel

personnel in possession of such status as to allow access to areas via a different (lower) level of screening

NOTE This status is usually achieved through security checks.

2.1.3 belongings

individual's personal possessions, which may include outer clothing, bags, portable electronic devices, wallets, keys, money, other carried items and **tools-of-the-trade** (2.1.30)

2.1.4 checkpoint

defined search point where people can cross a boundary from an open unscreened area to a secure area where threat items and other designated items are prohibited

2.1.5 client groups

different categories of persons requiring different levels of screening according to the risk they present

NOTE These may for example be staff, visitors, spectators, VIPs, contractors or skilled manual workers.

2.1.6 demand

rate at which an organization requires screening to be achieved

2.1.7 divest

process of removing items from a person to improve the efficiency and/or effectiveness of the screening process

NOTE Examples include the removal of outer clothing and pocket contents.

2.1.8 event

organized gathering of the public whether on payment or otherwise in the open air or under cover

2.1.9 explosive

energetic material or mixture – of improvised, commercial or military origin – that is capable of causing an explosion or incendiary effect

NOTE These can be powders, solids, slurries or liquids and include pyrotechnic compositions.

2.1.10 explosive device

device comprising explosive material and other components designed to provide an explosive or incendiary effect

NOTE Explosive devices come in many shapes and sizes. The explosive material could be a solid (for example sheet, stick, moulded block of regular or irregular shape), slurry, powder or liquid.

2.1.11 false alarms

alarms occurring in the absence of a threat item

NOTE False alarms should be distinguished from nuisance alarms. The latter may be triggered by objects that are not threat items, for instance, a metallic belt buckle may be legitimately detected whilst passing through a walk-through metal detector (WTMD).

2.1.12 malicious attack

deliberate attack or hoax designed to cause disruption, economic damage, physical harm, terror or distress

NOTE Such attacks will often be planned and premeditated.

2.1.13 manual search

search of a person, bag or other items conducted by hand by skilled security staff

NOTE 1 Manual search of people is often referred to as "hand search" and is known colloquially as a "pat-down".

NOTE 2 Manual search may contain a substantial visual inspection element.

2.1.14 non-regulated environments

environments where security checkpoints are not regulated by the Government

NOTE In the UK regulations apply to aviation, maritime and rail.

2.1.15 primary screening measure

initial screening of persons and/or belongings to check for the presence of threat items or other prohibited items

NOTE May use technology (typically high throughput/ low cost) or simple risk assessment (for example, screen only those with bulky clothing or large bags).

2.1.16 prohibited item

item deemed by an organization likely to pose a threat or have the potential to cause harm or disruption to its normal business and function

NOTE 1 Prohibited items may or may not be illegal.

NOTE 2 It may not be proportionate or cost-effective for a screening process to be designed to find all prohibited items; it may be acceptable for the process to focus on those representing the greatest risk to the organization.

2.1.17 recompose

recovery by an individual of their personal items and belongings after passing through a checkpoint screening process

NOTE Recompose is the opposite of divest (2.1.7).

2.1.18 refresher training

systematic and regular training programme to maintain and update previously achieved skills

2.1.19 resolution search

search usually carried out, following some trigger, with the expectation that a specific article may be found

2.1.20 risk

situation determined by the likelihood and impact of an incident arising from a particular threat scenario

2.1.21 screener

member of **authorized personnel** (2.1.2) who has acquired a competent level of performance at search/ screening tasks following training and assessment

NOTE Screeners are sometimes referred to as "searchers". The two terms are often used interchangeably outside this PAS.

2.1.22 screening search

search in which the principal aim is to determine whether a bag or person is free of certain **prohibited items** (2.1.16)

2.1.23 secondary screening measure

follow-up screening method or technology used when primary screening method has flagged a person/item for further search, which may be a more thorough search or alternative technology dependent on operational procedures

2.1.24 security screening

application of technologies and/or techniques to detect and/or identify prohibited items carried by individuals

NOTE It may not be cost-effective or proportionate for a screening process to detect all prohibited items; instead it should focus on detecting threat items presenting the greatest risk.

2.1.25 threat

ways and materials with which a **malicious attack** (2.1.12) may be carried out on a building, site, organization or people

2.1.26 threat item

explosive device (2.1.10), weapon or other **prohibited item** (2.1.16) that has the potential to cause harm, disruption or personal injury

2.1.27 threat level

indication of the likelihood of a **malicious attack** (2.1.12)

2.1.28 threat scenario

combination of a **threat item** (2.1.26), how and by whom it might be carried out, and the location and/or target

2.1.29 throughput

rate at which individuals and their belongings can be screened by a particular process using given resources

NOTE 1 Resources can include space, staff and equipment.

NOTE 2 Throughput is often stated as number of persons per hour, with measurements over shorter or longer periods scaled accordingly. It is sometimes referred to as footfall or flow-rate.

NOTE 3 When comparing throughputs potentially achieved by different screening processes it is important to understand, and account for, differences in resources expended.

NOTE 4 See also demand (2.1.6).

2.1.30 tools-of-the-trade

implements or materials normally carried by certain client groups to enable them to carry out their duties, for example, construction and maintenance workers (tools), chefs and caterers (knives).

***NOTE** There may be a need to allow some items normally classed as prohibited at a particular site (for example, knives, aerosols, gas cylinders) to enable certain client groups to do their jobs.*

2.1.31 weapons

items such as firearms (commercially manufactured, improvised or converted), ammunition, swords/knives or similarly sharp bladed objects, stab/spike implements and clubs/coshes

2.2 Abbreviations

For the purposes of this PAS, the following abbreviations apply.

CCTV	closed-circuit television
CPNI	Centre for the Protection of National Infrastructure
CT	computed tomography
CTSAs	police counterterrorism security advisers
EDS	explosives detection system
ETD	explosives trace detector
FAR	false alarm rate
HHMD	hand-held metal detector
ICE	Institution of Civil Engineers
IED	improvised explosive device
IMS	ion mobility spectrometry
IP	ingress protection
NaCTSO	National Counter Terrorism Security Office
NIJ	US National Institute of Justice
NILECJ	US National Institute of Law Enforcement and Criminal Justice
NOS	National Occupational Standards
Pd	probability of detection
RSES	Register of Security Engineers and Specialists
SIA	Security Industry Authority
TIP	threat image projection
WTMD	walk-through metal detector

3 Outline of process

The organization and/or its appointed security contractors should conduct a comprehensive assessment of risk (see Clause 4). This assessment should include:

- a) the consideration of the organization's vulnerabilities (see 4.1);
- b) the possible threats (see 4.2.2);
- c) the likelihood of a malicious attack (see 4.2.3);
- d) the potential impact (see 4.2.4) of such an attack;
- e) the recording of this information (see 4.3); and
- f) actions taken to manage or mitigate the risk (see 4.4).

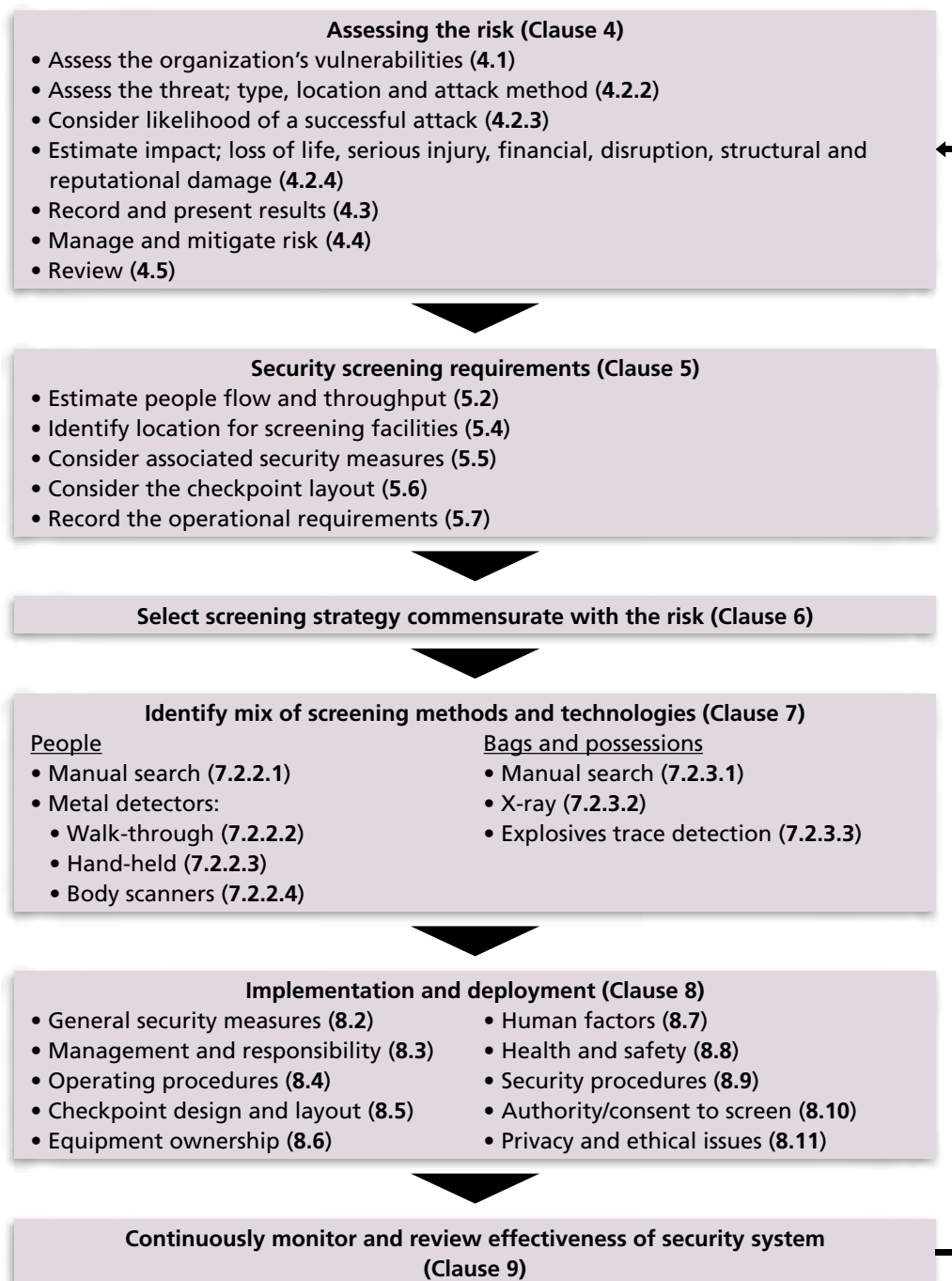
The organization should record the findings of the risk assessment, formally stating its requirements for security screening (Clause 5).

Based on its requirements, and if deemed necessary, the organization should identify appropriate screening strategies (Clause 6) and identify solutions in the form of security screening technologies and methods (Clause 7). These should be implemented accordingly (Clause 8) with regular review (Clause 9).

Ad hoc adoption of individual measures described in this PAS can lead to the implementation of an inadequate capability, or to unsafe practices. For these reasons the whole process should be followed if checkpoint screening measures are required.

The PAS 127 process is outlined in Figure 1 below.

Figure 1 – Summary of PAS 127 process



4 Assessing the risk

4.1 General

An assessment of the risk to the organization from person-borne explosives and weapons threat items is an essential first step in identifying the requirements for checkpoint screening. When completed, the risk assessment should provide answers to the following question: "How likely is this organization, operating at locations A, B and C, to be vulnerable to an attack or incident utilizing threat items X, Y or Z and what would be the impact of a successful attack?"

The risk assessment should be consistent with other organizational security policies and wider security risk assessments. The establishment of a checkpoint, if justified, should complement other pertinent physical security measures.

The organization should ensure that staff have the necessary knowledge and experience to conduct robust risk assessments. Where this is not the case it should seek expert support and/or appropriate training.

4.2 Risk assessment process

4.2.1 General

The organization should follow a three-stage process when conducting its risk assessment:

- a) a threat assessment of relevant threat scenarios;
- b) the likelihood of a successful attack should be considered for different threat scenarios explicitly taking into account existing security measures;
- c) the impact of the attack should be evaluated.

NOTE 1 *The risk assessment process outlined above is a good general starting point for most organizations. More complex methods are possible but it is likely that the key aims discussed here will still be relevant. The Institute of Risk Management website contains more information on risk assessment: www.theirm.org.*

The organization should note that risk assessments are not static and should be regularly re-examined.

NOTE 2 *For example, the nature of the threat can change as an organization's profile evolves, so that it becomes the focus of an attack.*

4.2.2 Threat assessment

The threat assessment should include details of the threat items of concern. The threat assessment should consider how and by whom the threat items might be carried and where they might be used. Each possible combination is called a threat scenario.

When making a threat assessment, the organization should consider the following factors, which can make an organization or event appear attractive as a target for attack:

- a) high profile of the building or venue, especially if it is of national or historic importance;
- b) government buildings;
- c) significant places of worship;
- d) major international events, especially if they have widespread media coverage;
- e) buildings or events attended by VIPs and/or royalty;
- f) The nature of an organization's business, as this can be a focus for protest groups.

Indirectly related factors that should also be considered include the presence of high profile and iconic buildings nearby, the activities of other businesses that share the same building, the activities of business supply chain partners, and recent events that may indicate that the threat environment is changing.

NOTE 1 *It is worth checking government websites given in the Bibliography periodically as useful sources of information with regard to threat assessment.*

The organization should inform the police in advance of any major events taking place, and clarify any legal obligations it may have with regard to event planning, operation and public safety.

NOTE 2 *The police may be able to advise on local issues that may influence the threat assessment and will be able to provide advice as to threat items likely to be encountered. Police counterterrorism security advisers (CTSAs) are resident within police forces and can provide specific information relating to the terrorist threat.*

Where the threat to an organization is likely to fluctuate over time as a result of external or internal factors, the organization should include in its risk assessment the concept of a threat level that can be used to help define differing levels of risk and response.

NOTE 3 *The threat level may be influenced by national threat levels. The UK has a national threat level system, which indicates the potential threat of a terrorist attack. See www.gov.uk/terrorism-national-emergency for more details. The five threat levels in this system are defined as:*

- a) *low – an attack is unlikely;*
- b) *moderate – an attack is possible, but not likely;*
- c) *substantial – an attack is a strong possibility;*
- d) *severe – an attack is highly likely; and*
- e) *critical – an attack is expected imminently.*

4.2.3 Likelihood of a successful attack

The organization should assess and record the likelihood of a successful attack given existing security measures for each threat scenario. The organization should then assign a numerical score from low to high (1 to 5 is typically used) to each threat scenario depending on what it considers to be the likelihood of a successful attack.

When assessing the likelihood of a successful attack, the organization should take into account that people carrying out malicious attacks often use reasoned approaches in calculating the personal risk involved in delivering a successful attack. This in part depends on the effectiveness of deployed and known security countermeasures. They may seek to identify and attack the less well-protected areas. The organization should therefore consider which areas may be considered as vulnerable.

4.2.4 Impact of a malicious attack

The organization should assess and record the impact of each threat scenario if it were to occur. The impact can be financial, loss of life and/or serious injury, and/or structural damage.

The organization should consider factors such as reputational damage, public outrage, disruption, and loss of confidence and business continuity. The organization should assign a numerical score to each threat scenario from low to high (1 to 5 is typically used) depending on the estimation of the impact of such an attack.

NOTE *For example, 5 = loss of life, major structural damage causing building operations to cease.*

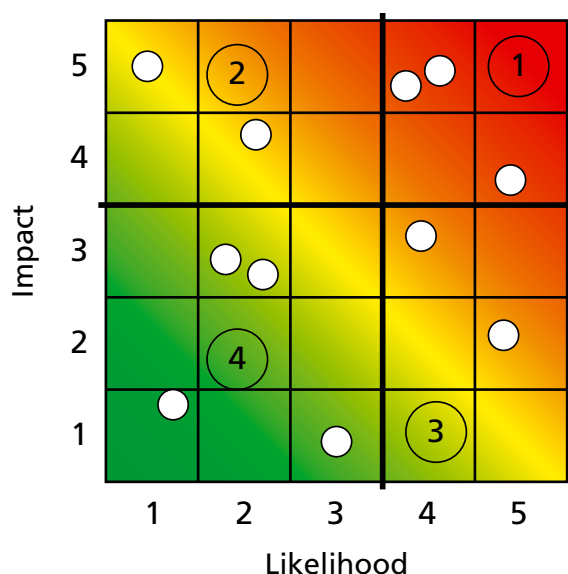
4.3 Recording and presenting the results

The organization should record the results for each threat scenario. The organization should produce a ranked list of risks to identify and inform risk management and mitigation. The organization should disseminate the information to those with a need to know in order to discharge their management responsibilities or to plan or operate the security processes. The organization should store the information securely and use version control, so that it is clear that the version filed is current.

The organization should plot the two separate scores on a graph similar to that in Figure 2.

NOTE *In this example taken from Protecting Against Terrorism, 3rd edition, CPNI, 2010 [1] the threat scenarios broadly cluster in four segments, with scenarios in the red segment (1) being relatively likely to occur and to have a high impact.*

Figure 2 – Plot of impact of a threat scenario versus its likelihood



4.4 Risk management and mitigation

When the risk assessment is complete the organization should take actions to allow the risks to be managed or mitigated in the following ways:

- a) adapt or change operating models: for example, limit or stop visitors, restrict bags and possessions carried or limit or control access to areas that could be attractive targets;
- b) accept: the risk is low so adapting or changing the operating model is not viable;
- c) protect: consider introducing checkpoint screening measures underpinned by clearly set out policies and procedures; these measures may use a combination of manual and/or equipment-based search techniques.

4.5 Risk assessment review

The organization should review its risk assessment regularly, after any actual or attempted malicious attack, or whenever changes internally or externally may lead to an increased risk of being targeted.

5 Checkpoint screening requirements

5.1 General

The organization's checkpoint screening requirements should be derived from:

- a) the risk assessment (Clause 4);
- b) an understanding of required/expected people flows through the entrances to the building or event venue (5.2);
- c) the locations available for screening (5.4); and
- d) associated security measures (5.5).

In the case of temporary checkpoints, for example at events, there are further requirements associated with the setting up and removal of the checkpoint (5.3).

The organization's screening and security measures should be appropriate and proportionate given the likelihood and type of threat to the organization. The organization's screening capability should be flexible; it should be able to cope with the need to increase the level of screening at times of heightened threat. The target levels for detection of specified threat items should be recorded, as should the false alarm rate tolerable for a given operation. Target levels for detection of specified threat items should be linked to the impact of a malicious attack (4.2.4).

5.2 People flows, throughput and belongings

The organization should develop and document an understanding of the demand for the screening process, ideally broken down by client group, and how this may vary over time. The organization should also understand the impact and acceptability of queues for screening and safety.

The organization should therefore consider the following:

- a) the type of building or event;
- b) existing and planned entrances and exits;
- c) the client groups using each entrance and the risk they represent, for example whether they are known staff, ticketed or un-ticketed visitors, or contractors with tools-of-the-trade that may present risks that need to be managed;
- d) the prevalence of objects and items typically worn or carried upon the person and within bags, and their suitability for screening. Examples may include bulky watches, belt buckles and liquids;
- e) the prevalence of objects such as bicycles, wheelchairs and mobility equipment, which may be difficult to screen or require additional screening resources;

