PAS 127:2014

Checkpoint security screening of people and their belongings – Guide






HM Government

bsi.

Publishing and copyright information

ISBN 978 0 580 79006 5

ICS 13.310

Publication history

First published February 2014

Contents

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 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**).

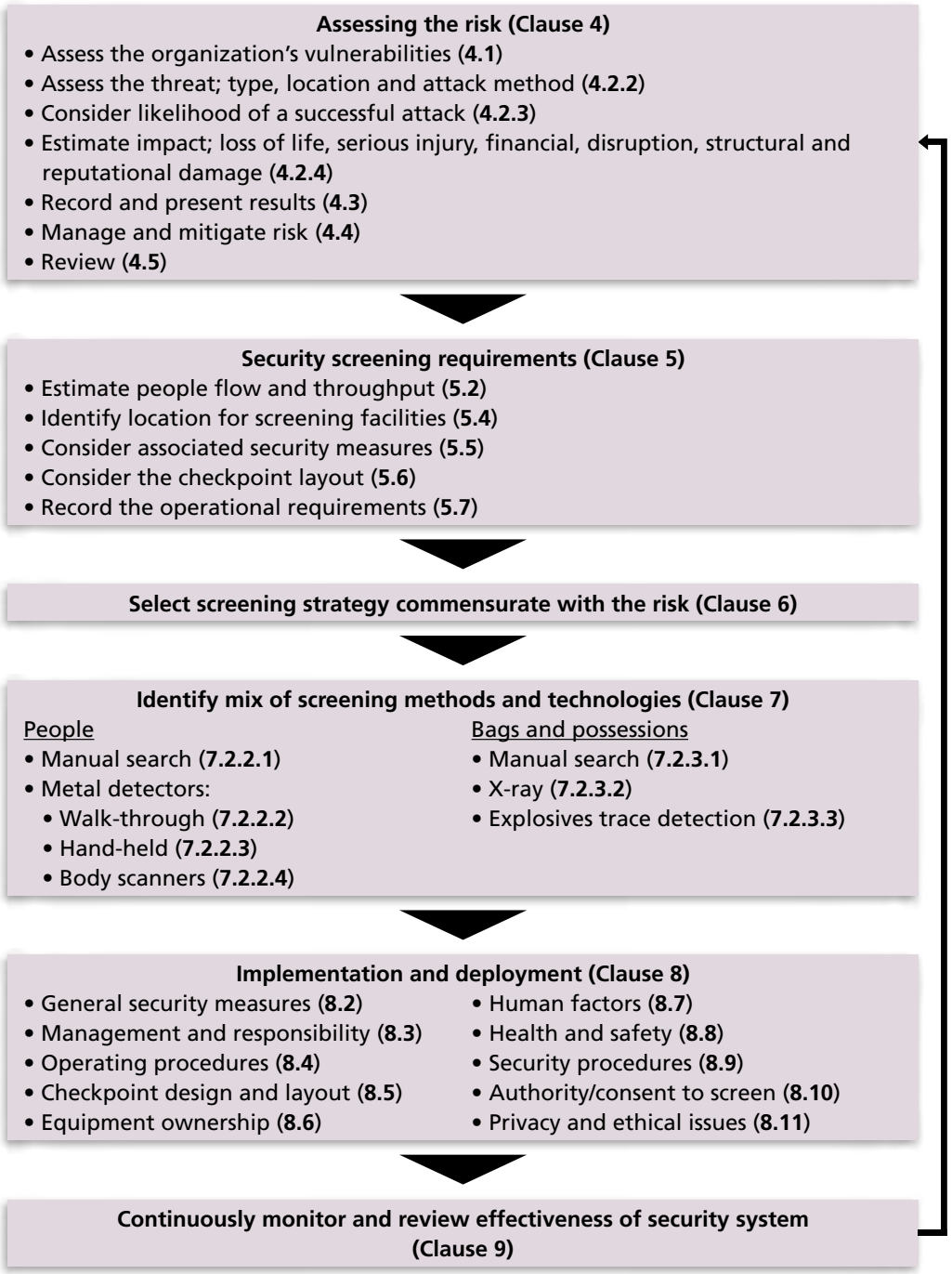
The organization should record the findings of the risk assessment, formally stating its requirements for security screening (Clause **5**).

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.*

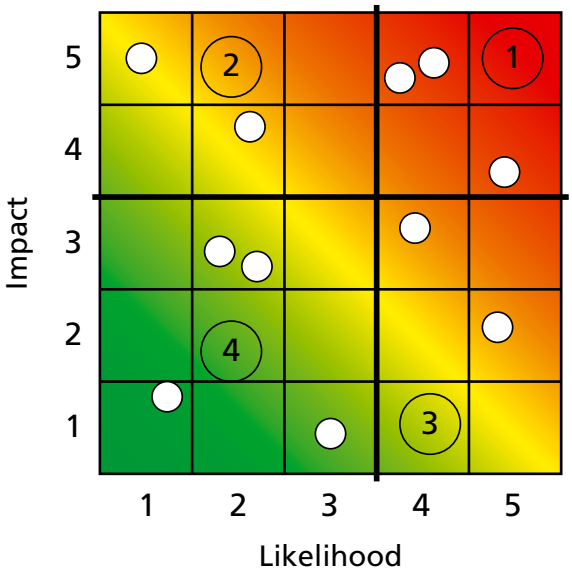
4.3 Recording and presenting the results

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;

f) the types of clothing anticipated and how this might change seasonally;
g) the average and peak flow of people through each entrance, with time of peak flow;
h) the acceptability and consequences of queues and delays.

The organization should arrange its screening capacity so that it is sufficient to cover both anticipated peak and average throughputs, and be able to accommodate fluctuations over time as well.

NOTE 1 *For example, people tend to wear more and be more reluctant to divest belongings on cold and/or wet days, which can slow down the screening process. Other factors that might cause an increase in the demands on the screening process include a raising of the threat level or an increase in the number of staff or visitors needing to be screened at particular times.*

The organization should inform people in advance of their arrival at a checkpoint that they will be screened, as people tend to take longer to pass through a checkpoint when they are not expecting to be screened.

A range of approaches may be used for advising clients about the screening process that they will encounter and the organization should consider this. Examples may include:

a) details given in advance by email or website as part of the ticket application process;
b) suitable signage; and
c) public address announcements providing instructions.

NOTE 2 *The formation of long queues at a checkpoint search facility is undesirable as queues can present an attractive target to a malicious attacker, as well as the obvious inconvenience to the persons being screened. Queues can also pose inherent safety risks such as:*

a) queues blocking exit routes;
b) safety of people within crowds at large sporting events (for example, football matches); or
c) queues spilling over into roadways.

NOTE 3 *Preliminary studies of time taken for individuals to pass through a similar checkpoint and forecasting people flows are often useful in the planning of security checkpoints.*

5.3 Temporary checkpoints

In the case of temporary checkpoints deployed at one-off or infrequent events, or at times of heightened threat level, the organization should consider the following:

a) time available for setting up and commissioning equipment before the operation and removing it afterwards;
b) space available for checkpoint screening equipment and queuing areas;
c) means of ensuring that individuals cannot bypass the checkpoint and avoid being screened;
d) requirements for power, lighting, and protection of staff and equipment from the weather;
e) transport requirements for equipment, for example, the need to pass through doorways;
f) sources of electrical and other interference, which may affect detection equipment;
g) stability of flooring and other temporary structures, both to accommodate likely loads of equipment and people, and to prevent false alarming of WTMDs, if deployed;
h) adequate training of staff assigned to temporary checkpoints.

NOTE *Points a) to h) above apply to all checkpoints but may be particularly pertinent when setting up temporary checkpoints.*

5.4 Location of screening facilities

In most situations the principal requirement for the location of a screening facility is one that allows sufficient space to conduct screening to a suitable standard for the anticipated throughput of people. In the case of buildings that may be targets for malicious attack, the location of a security checkpoint should be carefully considered with the aim of minimizing the impact of a blast. Generally, security checkpoints should be situated as far as practically possible from vulnerable targets. For example, locating checkpoints at the perimeter of a site rather than at the entrance to significant buildings may be advantageous but may not be practical. The organization should consult a suitably qualified security engineer to advise on its own particular building or site.

NOTE 1 *Suitably qualified engineers can be found in the Register of Security Engineers and Specialists (RSES) http://www.ice.org.uk/qualification-careers/Professional-Registers/UK-Professional-Registers/The-Register-of-Security-Engineers---Specialists.*

The organization should also consider the following factors when deciding on the best location for a checkpoint:

a) space constraints: ideally, the space available for the screening process should be sufficient to meet demand, i.e. to enable screening of the predicted volume of people at an acceptable rate and to the required standard. If this is not possible then some form of compromise will be necessary, for example, allocating more space, considering different processes and equipment or otherwise changing the screening strategy;

b) the use of adjacent rooms, floors and occupancy: the organization should understand the potential impact of an explosion on the use of adjacent rooms and floors;

c) the organization should have a clear and documented plan for evacuation in the event of a significant threat item being discovered in the checkpoint area. This plan should include a consideration of alternative exits. So, in the event of a threat item being discovered at a checkpoint, there should not be a single exit route that passes only through the checkpoint;

d) the size and weight of screening equipment such as X-ray machines and the required strength of flooring;

e) connectivity of power supplies and any data cables.

NOTE 2 *Further guidance on the design and location of checkpoints to mitigate the effects of blast can be found in Annex A and in Home Office Publication 16/13,* Guidance on Mitigation of Internal Explosions in Foyers and Entrances, *Home Office, 2013 [2].*

5.5 Associated security measures

The organization should only consider the implementation of checkpoint screening measures where the site has a suitably secure and controlled perimeter. Relevant security measures include the following:

a) fences, gates, doors, windows and other physical means of securing the perimeter;

b) access control measures such as policies regarding:

   1) who may enter, condition of entry (see **8.10**) and prohibited items;

   2) background checks;

   3) manual or automated systems for checking credentials or tickets at point of entry;

NOTE 1 *Communication of recommendations and restrictions (such as size and number of bags allowed, prohibited objects) should be done in advance if possible, especially where visitors are travelling some distance to an event.*

c) perimeter intrusion detection systems (PIDS) and CCTV systems;

d) a suitably trained and experienced guard force, operating these measures and able to respond quickly and effectively to any incidents or alarms.

NOTE 2 *This PAS addresses the screening of people and their possessions. The risks associated with all other items entering secure sites (for example, vehicles, bulk deliveries, mail and courier deliveries) should also be considered, as should appropriate screening measures to mitigate such risks.*

NOTE 3 *See also PAS 97:2012,* A specification for mail screening and security.

When a secure site is established, areas should be searched and cleared by trained security staff to determine that no previously emplaced threat items are present. A secure perimeter should then be maintained.

For security measures to be effective the organization as a whole should foster a healthy security culture. The organization should encourage a good level of awareness and vigilance in all staff regarding suspicious items and activities.

5.6 Checkpoint layout

NOTE 1 *Since every site is different, and the requirements for the screening operation will vary from one organization to another, it is neither possible nor appropriate to provide guidance on a standard checkpoint layout. It is important to remember that a poor checkpoint layout can have an adverse impact on throughput. There are a number of common themes and rules of thumb that have been developed and observed operationally. The most important consideration is the space required for the planned screening process.*

When planning the layout of a checkpoint, the organization should ensure that there is sufficient space to:

a) accommodate and operate specific equipment;

b) accommodate staff;

c) perform manual screening processes; and

d) handle the expected volumes of people to be screened while maintaining control of the process.

NOTE 2 *These factors are discussed in more detail in* ***8.5****.*

NOTE 3 *It is important to consider layout in terms of implementing the adopted screening strategy using the selected technologies and methods. These are discussed in Clauses* ***6*** *and* ***7****.*

In addition, organizations should apply "good housekeeping" rules to checkpoints; for example, clutter-free environments are essential in maintaining efficiency.

5.7 Recording the operational requirements

The organization should formally record its requirements for security screening in sufficient detail to enable unambiguous implementation either by its own staff or by a contractor. This record should include the following items:

a) a summary of the organization's understanding of the demand for the screening process, such as flow of people by client group, and how this may fluctuate over time;

b) a summary of the threats that the organization faces and the relative importance of detecting each threat item;

NOTE *The relative importance of detection of different types of prohibited items may be categorized, for example, according to whether they are deemed "essential to detect" or "desirable to detect".*

c) the desired levels of detection and tolerable false alarms;

d) how alarms from the screening process are to be managed and resolved;

e) recognition of complementary security measures (for example, perimeter security and access control measures) and how the screening process needs to interface with these;

f) any changes made as the result of a formal review of screening procedures;

g) layout and location constraints of a checkpoint and whether these are permanent or temporary.

6 Screening strategies

6.1 General

Having identified its operational requirement for checkpoint security screening, the organization should develop a strategy for how that requirement will be met. This screening strategy should deliver a proportionate screening solution, balancing risk reduction with the impact on the people being screened and the operation of the organization.

NOTE 1 *The impact may encompass delay, inconvenience, or perceived or actual invasion of privacy or civil liberties (see **8.11**).*

Many screening strategies will consist of primary screening measures and secondary and/or resolution measures. Manual and/or equipment-based search techniques may be used.

NOTE 2 *Screening measures may be based upon risk assessment (for example, checking credentials, with trusted staff then not subjected to further screening; bags/possessions above a certain size being subject to screening).*

The organization should consider the following when selecting a screening strategy that addresses the operational requirements:

a) what prohibited items are essential and/or desirable to detect;

b) who will be screened and what belongings they are likely have (see **5.2**);

NOTE 3 *It can be helpful to categorize the people to be screened into client groups, and consider the risks associated with each group. It may be appropriate to use a different screening strategy for different groups, depending on the relative risks they pose. A key factor in assessing the risk is the information or knowledge that the organization has of the client group. For example, staff should pose a lower risk than members of the public. Another important factor will be the quantity and type of possessions that particular client groups may bring.*

c) demand for the screening process (see **5.2**);

NOTE 4 *Consideration should be given to how demand may vary over time (for example, daily peak hours, seasonally, or as the organization grows).*

d) how the screening will be conducted (such as primary or secondary measures);

e) what techniques and technologies will be used (see Clause **7**);

f) whether and how search and/or screening measures are applied randomly;

g) how screening measures may be enhanced at times of heightened threat;

h) other requirements and constraints (for example, financial, space, equipment, staff).

6.2 Implementation

The organization should subject all people and belongings entering a site to the required standard of screening. This is the screening strategy that offers the highest level of assurance. In practice, costs, resource constraints (space, equipment, staff) and demand may often prevent this.

If screening all staff and visitors is not feasible, the organization should consider the following possible approaches (in approximate order of decreasing assurance provided):

a) regulating the demand for the screening process, for example, by staggering arrival times of visitors or staff;

b) screening everybody to the same, but reduced, standard (such as focusing only on those threat items deemed essential to detect);

c) using risk-based prioritization of screening resource (such as assessing risk by client group, which might lead to a decision to screen all visitors routinely, but not staff; or screening only people wearing bulky clothing, or bags/possessions larger than a certain size);

d) applying screening measures to a random selection of clients.

NOTE 1 *Applying screening measures to a random selection of clients can have deterrence value where 100% screening is impractical.*

The organization should ensure that the random selection of clients to be screened is truly random (i.e. unpredictable), so that it cannot be exploited or lead to allegations of discrimination. The organization should consider the effectiveness of the screening process in deciding what the level of unpredictability should be.

NOTE 2 *Given its limitations, random application of screening measures is most appropriate for low-risk client groups or supplementing baseline measures (for example, at times of heightened threat).*

NOTE 3 *A predictable screening process presents a weakness that may be exploited by those with malicious intent.*

Whatever strategy is adopted, the organization should aim to utilize fully available resources (staff, space, equipment). For example, supplementary screening measures such as manual search of people and/or bags and possessions should, as far as possible, be used whenever staff are free to apply them. They should not only be deployed in cases where an alarm from a primary screening measure requires their use.

6.3 Managing fluctuations in demand

The organization may need to adapt screening measures in response to fluctuations in demand. The organization should have a clear policy and supporting procedures on what action to take in the event that peak demand outstrips screening capacity.

6.4 Future proofing

The organization should ensure that its screening strategy is sufficiently flexible to address both current and likely future requirements, arising, for example, from the growth of the organization or changes in the threat.

7 Technologies and methods

Table 1 – Common security screening methods and technologies

Method	Objects detected	Alarm resolution	Notes
		People screening	
Manual search	All carried objects: • explosives; • guns; • knives; • other suspicious items.	Often used to resolve WTMD or other alarms.	Requires no technology. Effective if carried out thoroughly. Staff intensive and time consuming. May be seen as invasive. Hand search usually same gender only. Disguised threat items and threat items hidden in other objects may not be identified. Health and safety issues when sharp items may be present.
WTMD	Large and small metal items: • guns; • metallic knives; • metal components of explosive devices.	Manual search or HHMD required to resolve alarms. Requires separate checking of divested carried objects.	Fast and automatic, but requires alarm resolution. Does not detect non-metallic threat items. Sensitivity can be adjusted. Potential for high nuisance and false alarm rates. Some WTMDs indicate height above ground of metallic items. Requires correct set-up, on stable floor away from moving metal objects.
HHMD	Large and small metal items: • guns; • metallic knives; • metallic components of explosive devices.	Can be used as part of WTMD alarm resolution process.	Slower than WTMD for primary screening. Can be set to detect very small metal threat items that are then resolved by thorough inspection. Does not detect non-metallic threat items. Requires correct operator use.
Body scanners, for example, millimetre wave imagers and portals, X-ray backscatter imagers	Large and small concealed objects of all types, including: • explosives; • guns; • knives; • other suspicious items.	Directed manual search required to resolve alarms.	Detects metallic and non-metallic threat items. High purchase and running costs compared with other techniques. Locates suspicious objects to facilitate alarm resolution. Throughput relatively slow. Privacy issues need to be taken into account, however, newer automated systems do not display actual images. Requires comprehensive operator training. Perceived safety risk with X-ray backscatter technologies.

Table 1 – Common security screening methods and technologies *(continued)*

Method	Objects detected	Alarm resolution	Notes
		Bag/possessions screening	
Manual search	All contained objects: • explosives; • guns; • knives; • other suspicious items.	Often used to resolve X-ray or other alarms.	Requires no technology. Effective if carried out thoroughly. May be staff intensive and time consuming. May be seen as invasive. Disguised threat items and threat items hidden in other objects may not be detected. Health and safety considerations for sharp items. Thoroughness and speed can be tailored according to requirements.
X-ray	All contained objects: • explosives; • guns; • knives; • other suspicious items; • disguised threat items and threat items concealed inside other objects.	Requires an alarm resolution process such as manual search of suspect bags/possessions.	Requires specially trained operators. Requires regular safety checks.
Explosives trace detection (hand-held or desktop)	Explosives (indication that a person/bag may have been in the presence of traces of explosives or other contaminated items). Explosives trace detector (ETD) systems may detect explosives particulate traces and/or vapours.	Can be used as a secondary screening technique following X-ray bag screening to increase confidence that no explosive threat items are present.	Generally requires collection of particulate material from surfaces or sampling of airborne vapours for analysis in the ETD system. Usually applied to bags and possessions. ETD can also be used to screen people by taking swabs of personal items that are frequently touched, such as mobile phones or wallets. A trace detection alarm does not necessarily mean that a bulk quantity of explosives is present. ETD systems do not address non-explosive threats. Requires specially trained operators.

7.1 General

The previous clauses have emphasized that organizations should define their operational requirements and select screening strategies. This clause introduces potential solutions that may be used to meet the operational requirements for the screening strategies.

Security screening at a checkpoint can be carried out using manual searches, a variety of types of detection and/or identification equipment, or both. In all cases, equipment should be used by trained operators and may need to be supplemented by manual processes for the resolution of alarms. The organization should provide training so that its staff have the necessary skills to operate equipment and perform manual processes (see **8.7.2**). After initial training, the

organization should provide regular refresher training for staff to ensure that they maintain their skills.

NOTE 1 *Usually a combination of equipment and manual processes is required to provide a comprehensive detection solution.*

Screening should be carried out using established equipment/technologies and methods selected to meet the requirements.

Commonly used technologies and methods are summarized in Table 1. A brief description of the means of operation of each technology is given in **7.2**.

NOTE 2 *In some instances the use of specialist detection technologies may be appropriate. Some of these less well established technologies are discussed in* ***7.2.3.4.***

7.2 Screening technologies and methods

7.2.1 General

The description of technologies and methods presented here and in Table 1 gives a brief overview. It has not been possible within the scope of this document to provide a comprehensive summary of all aspects. For this reason, expert advice should be sought on the suitability of particular methods, technologies or products to address a screening requirement. Similarly, the guidance here should not be used as a substitute for full and detailed training and validation of security operators in the specific methods.

7.2.2 People screening

7.2.2.1 Manual person search

Manual search involves the use of the physical senses to detect threat items concealed on the body or within carried items. Permission from the individual to be searched should be sought in advance and the process explained to them. Manual searching has the potential to produce conflict situations so this activity should be properly supervised.

NOTE 1 *Manual search of carried items is covered in* ***7.2.3.1.***

NOTE 2 *Though commonly referred to as "manual search", such techniques typically rely on visual inspection as well as the sense of touch.*

There are generally two types of manual search:

a) screening search: a primary screening measure in which the principal aim is to determine if a person is carrying prohibited items; and

b) resolution search: a secondary screening measure, usually carried out following some trigger, with the expectation that something is likely to be found. Depending on the primary screening measure that has identified the need for further investigation, the secondary resolution search may need to cover the whole body, or just a particular area.

The organization should ensure that all searches, whether screening or resolution, are conducted systematically so that no areas are missed.

When conducting a manual search on an individual, an operator should feel for objects through that individual's clothing by using a gentle sliding motion of their hands and applying sufficient pressure to detect objects through the clothing.

In many screening processes it is advantageous to ask individuals to divest themselves of outer clothing (for example, coats and jackets) and body-worn items such as belts and pocket contents. These items can then be screened separately, for example, manually (**7.2.3.1**) or in an X-ray machine (**7.2.3.2**). Divested items should be kept within sight of their owners.

NOTE 3 *Manual search is most effective and efficient when the individual's outerwear and pocket contents have been divested, though the need to inspect these items separately can have an impact on the efficiency of the overall process.*

The organization's decisions regarding the extent of divesting should reflect the overall requirements of the process (such as throughput and detection performances).

The thoroughness of, and hence time taken for, the manual search process should be matched to the categories and sizes of threat items it is required to find.

Manual searches are physically demanding for staff, so the organization should design the search process so that the risk of performance degrading over time (see **8.7.5**) is minimized. In order to alleviate the adverse effects of loss of concentration manual screeners should rotate their duties at regular intervals during a shift. The length of interval depends on the nature of the screening task and may be adjusted accordingly.

NOTE 4 *This principle applies to all staff deploying the various security methods outlined in the whole of this clause.*

The organization should put in place policies and procedures for screening minors, the mobility impaired and other disabled people, as well as those with religious beliefs or particular medical conditions that may impact on the screening process. For major screening operations, dedicated private search areas should be available within, or in very close proximity to, the checkpoint. For smaller, less pressurized operations, appropriate provision should be made for private searches to be conducted.

NOTE 5 *Detailed secondary searches, or resolution searches, where an individual is strongly suspected of carrying a prohibited item, include strip searches and intimate searches. These are beyond the scope of this current PAS. These searches should only be conducted in a discreet environment by fully qualified and authorized practitioners such as trained police officers.*

For adult clients, it is good practice for a search to be conducted by a person of the same gender as the person being searched. It is preferable for children to be screened by female screeners. Where no screener of the correct gender is available, alternative non-contact approaches can be used (such as HHMDs), instead of manual search.

The organization should consider the health and safety of its screening staff conducting manual searches, and in particular whether, and under what circumstances, it should mandate that gloves be worn. The health and safety benefits of wearing gloves should be weighed against the slightly reduced search effectiveness that may arise if gloves are worn.

Persons may be carrying more than one suspicious or prohibited object. Searches should be conducted in a systematic manner that takes account of this, resuming the search after an item has been found until the whole body has been covered. Screeners should be aware that an innocuous object may be used to distract attention from a second, more harmful, object.

NOTE 6 *Some types of equipment give an indication of the location of concealed items. This may permit a manual search targeted on just one or two locations, rather than the whole body. If the equipment is unable to give locations of multiple objects, then it may again be necessary to re-screen a person with a metal detector or body scanner after an object has been divested in order to confirm that no further objects are concealed.*

NOTE 7 *Where a manual search has been used to resolve a metal detector or body scanner alarm, it may be beneficial to re-screen a person (with the metal detector or body scanner) in order to confirm that no further objects are concealed. Such an approach should be reflected in the organization's operating procedures for the screening process (see **8.4**).*

7.2.2.2 Walk-through metal detectors

NOTE 1 *A walk-through metal detector (WTMD) produces a changing magnetic field that induces electric currents in ferrous or non-ferrous metallic objects passing through it. The sensitivity can be adjusted to detect small or large metallic objects, depending on the requirements of the screening process. This can have a significant impact on throughput. WTMDs should be certified by their manufacturers as safe to use with implanted medical devices (such as pacemakers). Clause **B.2** contains synopses of relevant standards for WTMDs.*

The organization should follow the manufacturer's instructions to set the WTMD's sensitivity to a level that achieves an acceptable compromise between threat detection and throughput for the particular application.

Many WTMDs have a random alarm function and, if so, the organization should consider how this might be used to enhance its screening processes by enabling random screening for other prohibited items (see **6.2**).

When using WTMDs as a screening method, the screener should ensure that the client has divested all but the smallest metallic objects prior to passing through the WTMD. Divested items should be screened separately. The operator should ask each individual to walk slowly through the arch of the WTMD. The operator should resolve any alarms by manually searching the associated individual (see **7.2.2.1**) or by the use of a hand-held metal detector (HHMD) (see **7.2.2.3**). The number of screeners deployed to conduct these various tasks should be sufficient to meet the needs (for example efficiency, effectiveness and safety) of the screening process.

If individuals with implanted medical devices, artificial joints or other prosthetics voice concerns that the normal operation of these may be affected by a WTMD, the operator should offer manual search as an alternative. If appropriate, any resulting manual searches should be conducted in a private/discreet search area.

Operators should encourage clients to divest all outerwear, carried items or pocket contents, whether metallic or not as these can still represent a threat and will also impede any manual search required to resolve a WTMD alarm.

When designing the checkpoint, the organization should ensure WTMDs are kept away from large moving metal objects, such as doors or escalators, as these can affect their performance.

Many WTMDs are sensitive to electromagnetic interference and therefore the organization should also ensure that they are kept away from electrical equipment liable to produce large spurious electromagnetic fields.

The organization should mount its WTMDs on a solid stable surface and install them according to the manufacturer's instructions.

NOTE 2 *A WTMD mounted on loose temporary flooring will be susceptible to vibrations caused by passing pedestrians and is likely to generate a large number of false alarms as a consequence (see **8.5**).*

7.2.2.3 Hand-held metal detectors

NOTE 1 *Hand-held metal detectors (HHMDs) work on the same principle as WTMDs. They have a localized region of sensitivity and can be used to conduct a full search of a person as an alternative to a full manual search, or to localize and resolve alarms after a WTMD has indicated the presence of a metal object. HHMDs can be used to detect and localize small metallic objects.*

The operator should ask the individual being screened to adopt a pose with their legs slightly apart and arms stretched downwards forming an "A" shape with the rest of the body.

NOTE 2 *Such a posture takes up less space than if arms are held straight out sideways. Arms down to the side limits a person's ability to attack the screener.*

Searches using a HHMD should be conducted by the screener in a systematic manner so that the whole of the body of the individual being searched is screened front and back. If the HHMD is being used in a secondary resolution search then only the area of interest on a person needs to be covered. The HHMD should be operated in accordance with the manufacturer's instructions and operators should be given appropriate training in this.

If individuals with implanted medical devices, artificial joints or other prosthetics voice concerns that the normal operation of these may be affected by a HHMD, the operator should offer manual search as an alternative. If appropriate any resulting manual searches should be conducted in a private/discreet search area.

7.2.2.4 Body scanners

NOTE 1 *Body scanners are able to detect metallic and non-metallic objects that are concealed under clothing. Older systems typically produce images for an operator to examine for anomalies. As the images can be perceived as being invasive of the privacy of the individual being screened, there is a trend towards automated threat recognition software and other measures, removing the need for full images to be inspected.*

NOTE 2 *In some body-scanning systems ionizing radiation is used. There are public concerns over the safety of X-ray based techniques. See* ***B.3,*** X-ray standards *for more details.*

NOTE 3 *Due to their high cost, body scanners, as of publication, have not yet achieved widespread use.*

There are generally two categories of body scanner. The first category includes millimetre-wave and X-ray backscatter portals and requires the cooperative participation of the individual. When these types of scanners are used the screener should ask the individual to divest their outerwear (such as coats, jackets or bulky jumpers), headwear and pocket contents for separate screening.

The screener should then ask the individual to enter the body-scanning area and adopt a suitable position in accordance with the manufacturer's recommendations. Images are recorded from the front and back. In some systems this may require the individual to rotate slowly or adopt a second standing position 180° to the first. Body scanners are typically able to screen between one and five individuals per minute.

NOTE 4 *The second, less well-established category includes stand-off or walk-through equipment, which requires less cooperation from the individual and may be used in situations where divesting clothing is not possible. The performance of these is intrinsically linked to the size and location of the threat item being screened for and the time available.*

Where an imaging technology is chosen in which the image quality could give rise to privacy concerns, the organization should, if at all possible, use automated threat detection functionality to remove the need for operators to view actual images of the people being screened. Where that is not possible, the organization should carefully consider its policies and processes to minimize the impact on clients' privacy. For example, the organization should consider whether images should be viewed remotely and/or by a screener of the same gender as the client, and under what circumstances (for example, in response to an incident) images should be stored.

In cases where there are cultural, religious or other privacy sensitivities, the organization should consider offering an alternative to the use of body scanners, such as manual search.

7.2.3 Screening of bags and possessions

7.2.3.1 Manual search

This method requires no technology and can be effective in finding smaller threat items if conducted thoroughly. A disadvantage is that it is labour intensive, especially where bags are large, densely packed and/or contain a large number of items. Depending on what combination of screening methods are used, bag searches can be considered to be primary screening searches or resolution searches. The level of searching, and the time spent, should always be matched to the type and size of the threat item being sought.

In a resolution search, for example after the X-ray reveals a suspicious item, the screener should remove the contents of the bag item by item until they are confident that no threat item remains in the bag. The screener should closely inspect each item removed. The screener should also carefully examine the bag itself for any signs of tampering such as cuts, new material, fresh stitching or unstitching, unexpected weight and uneven balance that may indicate the presence of concealed threats.

A screening bag search may be the only screening method deployed. It may be conducted relatively quickly as it does not usually require the entire bag to be emptied. This method is often deployed in situations of high throughput, such as sporting events.

The organization should have a clear policy regarding whether the bag is repacked by the screener or by the client. When the screener repacks the bag they should

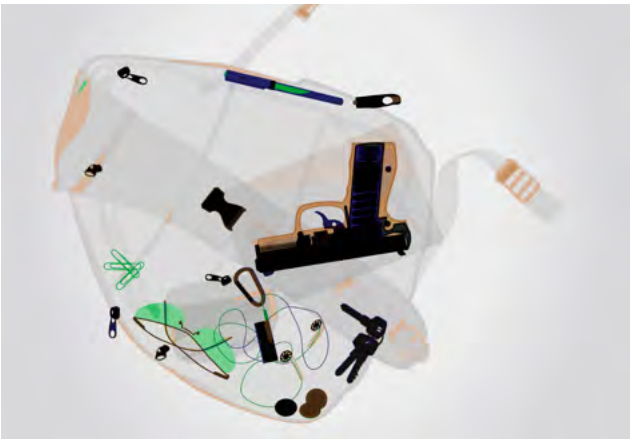
repack the bag and return it to the individual in the same condition as it was prior to the search.

Staff should be vigilant whilst carrying out a bag-searching task. They should be aware that multiple suspicious items may be present in a bag, so should continue searching to completion after finding and inspecting an item(s) of concern.

Staff should also be aware of the health and safety risks associated with manual bag searches, in particular the possible presence of sharp items (scissors, needles, knives, etc.). Before starting to search a bag, the screener should ask the client whether it contains anything dangerous. The use of gloves should be considered, noting that gloves thin enough to enable an effective search are unlikely to provide significant protection against sharp objects.

Manual search of items such as wheelchairs and pushchairs may also be necessary. In these cases it should be remembered that the wheelchair constitutes the personal space of the occupant and the screener should recognize this. The screener should explain the search process to the individual and be methodical, ensuring that areas are not missed.

When searching items such as wheelchairs and pushchairs, particular care should be taken to ensure that the search is completed in a systematic manner. In particular, care should be taken to ensure that all bags and other items carried or stowed on the wheelchair or pushchair are removed and searched in their own right.



7.2.3.2 X-ray

NOTE 1 *X-ray technology can be used for screening bags, outer clothing or other possessions such as mobility aids that may be used by mobility-impaired people. X-rays transmitted through a bag are attenuated by differing amounts according to the differing densities of the contents of the bag. Hence an X-ray image of the bag and its contents can be formed enabling threat items of a distinctive shape to be detected.*

NOTE 2 *X-ray machines vary considerably in sophistication from simple manually operated equipment to advanced computed tomography-based systems that produce 3D images. Most X-ray systems are "dual energy", which enables a degree of materials discrimination, for example, to discriminate between organic materials such as explosives, and metallic objects such as guns. As X-rays penetrate through material, X-ray screening provides an effective means of detecting threat items that have been concealed within other objects. Some of the more advanced machines have automatic explosives detection capability.*

NOTE 3 *A typical X-ray machine for bags has screening tunnel dimensions of approximately 0.6 m wide by 0.4 m high.*

When X-ray screening is used, an individual's divested items (outerwear, pocket contents, etc.) should be placed in a tray along with their bag on the X-ray machine's conveyor belt.

These items enter the X-ray machine through lead curtains. An image is obtained for each tray and bag. A trained X-ray operator should view each image and allow objects to pass sequentially if no threat item is observed.

NOTE 4 *Divesting and recomposing can cause significant delays to the X-ray screening process. Where high throughputs are required, it may be advantageous to encourage people to divest their pocket contents into their bag or outerwear while queuing, rather than depositing their pocket contents loose into a tray on reaching the front of the queue.*

NOTE 5 *Depending on the sizes and types of threat items the process is required to detect, and the complexity of bags, it may be necessary to remove certain items from bags (for example, larger electronic devices such as laptops, liquids) for separate X-ray inspection.*

X-ray systems are only as good as the operators using them. Operators should be trained comprehensively, and assessed, in the safe operation of the X-ray machine, identification of threats in X-ray images, and how to respond to threats. Periodic continuation training should be provided to maintain competence and also to keep abreast of changes in the threat.

NOTE 6 *Threat image projection (TIP) is a feature now commonly available on baggage X-ray systems.*

Periodically, the system superimposes the image of a threat item, such as a gun, in an image of a bag or other item. The operator has to detect the object and press a button to register that it has been seen. TIP acts as an aid to training and helps to keep the operator alert. It can also be used as a performance-monitoring tool.

The organization should consider whether to use TIP. Where TIP is used, the threat item libraries should be chosen to represent the threats that are to be detected in the particular checkpoint operation. Similarly, TIP system settings (including frequency of insertion) should be chosen to meet the needs of the organization's screening operation. If necessary the organization should seek advice.

NOTE 7 *The majority of available TIP threat item libraries have been developed for aviation security threats and may not be entirely suitable for other applications.*

7.2.3.3 Explosives trace detector

NOTE 1 *Explosives trace detectors (ETDs) can detect minute amounts of explosives residue, which can be found on items as a result of contact with bulk explosives (or other contaminated items) or airborne vapours emanating from concealed bulk explosives. Whether explosives traces are likely to be present as particulate residues or airborne vapours largely depends on the properties of the explosive – some will be more readily detected as particles and some as vapours.*

ETDs are generally configured to accept samples of only one of these two forms (vapours or particulate residues). However, some systems can be reconfigured easily, but not quickly, to operate in either mode. ETDs can be hand-held or bench-top instruments and employ a variety of different technologies, the most common of which is ion mobility spectrometry (IMS).

NOTE 2 *As with manual searches, ETDs can be used either as a primary screening tool for certain items (for example, items that are too large for X-ray screening) or as a secondary screening tool for the further investigation of items that have been identified by the primary screening method as being of concern and/or cannot be deemed clear.*

Methods of operation can differ from system to system. ETD equipment should always be operated in line with the manufacturer's instructions. However, in general, sampling of particulate residues should be conducted by wiping a swab over the target surface, focusing on areas that are likely to have been touched or handled and where it could be possible to conceal explosives. Vapour samples should normally be taken from within or in close proximity to items or enclosed voids that are not easily searched by other means.

To ensure ETD equipment performs to manufacturer specifications, regular performance testing and routine maintenance is required and should be undertaken according to the manufacturer's instructions. Equally, staff should receive training in the operation and maintenance of the equipment as well as in the organization's operating procedures, which should specify the action to be taken on encountering an ETD alarm (see **8.4** and Annex C).

An alarm on a trace detection system should only be used to direct further searches. If an ETD is used as a primary screening tool then the secondary (resolution) screening method should be employed. If an ETD is used as a secondary screening tool then any alarms should be followed by a thorough manual search.

NOTE 3 *The interpretation of ETD alarms and therefore the subsequent actions to be taken depend on the mode of operation (particulate or vapour) and how ETDs fit into the wider screening process (that is, whether it is used as primary or secondary screening). The detection of explosives particulate traces may indicate that there are threat quantities of concealed explosives present or that the item or person being screened has recently been in contact, legitimately or not, with explosives or other contaminated items. The detection of explosives vapours generally indicates the nearby presence of bulk explosives. However, in both modes of operation ETDs can suffer from false alarms caused by innocuous (non-explosive) chemicals that the equipment cannot distinguish from explosives.*

NOTE 4 *ETD alarms resulting from the detection of explosives traces from legitimate contact with explosives (for example, military, mining, demolition) are generally referred to as "nuisance alarms".*

Some ETDs contain small radioactive sources. These are low activity sources and do not pose a health hazard to operators or clients. However, they should be managed in accordance with safety regulations for the handling of ionizing radiation.

NOTE 5 *Attention is drawn to the Ionising Radiations Regulations 1999 [3].*

7.2.3.4 Other detection technologies and techniques

NOTE 1 *A variety of other detection technologies and techniques are also available, but are excluded from detailed discussion in this PAS as at the time of publication they are not widely used for screening people and their belongings. These alternative technologies and techniques include the following:*

a) systems capable of detecting threat items and contraband concealed inside the body, such as specialist metal detectors and low-dose transmission X-ray systems;

b) explosives detection dogs and handlers (canine explosives detection). The organization should refer to BS 8517-2:2010, Security dogs – code of practice for the use of dogs *(**B.4** gives a brief synopsis);*

c) passive magnetometers for the detection of guns, knives and person-borne improvised explosive devices (IEDs) containing metallic shrapnel;

d) high performance X-ray systems with automatic explosives detection capabilities;

e) bottle scanners and other liquid explosives detection systems;

f) stand-off threat detection systems;

g) explosives (and drugs) trace detection portals;

h) shoe scanners.

Organizations should ensure before purchase that security equipment meets their specific requirements.

NOTE 2 *As of the publication of this PAS, there are no formally recognized UK standards for testing the capability of screening equipment outside of aviation applications. Whilst equipment may have been tested by government or other bodies for a particular application, this does not necessarily mean that it will address the specific requirements that a particular organization may have.*

7.2.3.5 Fraudulent equipment

Designers of checkpoint security systems should take steps, including seeking advice from experts, to avoid the inadvertent deployment of fraudulent equipment that has little or no detection capability.

7.2.4 Selecting detection equipment

Once the organization has ascertained its operational requirement for checkpoint security screening and identified its favoured screening strategy and potential technological or manual solutions, there are three steps that it should undertake when considering the procurement of appropriate equipment.

a) Identify the general type of equipment required (for example, X-ray machine capable of screening small bags/possessions; walk-through metal detector capable of temporary deployment outdoors).

b) Identify a selection of commercially available solutions addressing the requirement.

c) Weigh up the respective merits of these possible solutions for the intended application, considering points such as:

- actual performance, as evidenced by independent equipment testing, at detecting key threat items relevant to the application under typical operating conditions;
- purchase or leasing cost of the equipment;
- anticipated lifetime of equipment;
- staffing costs (including training) given anticipated use;
- costs and timescales for maintenance and repair;
- anticipated cost of consumables, such as gloves, ETD swabs, batteries;
- mains and/or battery power options;
- power consumption and cost of electricity;
- size and mass;
- portability/mobility/ease of redeployment;
- ingress protection (IP) rating;
- any other installation or operating constraints, for example, proximity to metal objects;
- existence of established software/calibration settings relevant to the intended application;
- existence of equipment-specific training packages relevant to the intended application;
- potential to address possible future requirements;
- health and safety issues (for example, use of ionizing radiation).

NOTE *Outside of regulated applications, such as aviation security, there are no lists of "approved equipment" because the suitability of a piece of equipment will depend very much on the requirements of a particular application. Conversely, equipment approved for aviation security may not be optimal for other applications.*

7.3 Combining detection technologies and methods

The checkpoint screening system should be designed to achieve the required screening performance by using an appropriate combination of methods. Table 2 lists the common combinations of screening methods. Specialist screening technologies and methods can be used to supplement the combinations outlined in Table 2 or independently, if that meets the organization's screening requirements.

Table 2 – Common approaches to combining person search and search of bags/possessions, with example applications

		Bags and possessions search	
		Manual search	**X-ray screening (with manual resolution)**
Threat items addressed		Has the potential to detect any threat items, but may struggle to find well-disguised or concealed objects; procedure and thoroughness can be tailored to the threat; having a suitable work-surface to unpack bag contents onto will aid the efficiency and effectiveness of the search	Has the potential to address any threat items, including well-disguised or concealed items; process and equipment used can be tailored to the threat and to the size and complexity of items being screened
Throughput considerations		Throughput depends significantly on the quantity and size of bags/possessions and size and types of threat items to be detected; easily scalable to match varying demand	Throughput depends significantly on the efficiency of divest/preparation and recompose steps, and to a moderate extent on the complexity of objects being screened and the size and types of threat items to be detected
Staffing considerations		Staff intensive but limited training required	Specialist X-ray training required (with regular refresh) which should be relevant to the application (for example, with regard to bag type and complexity, and threats)
		▼	▼
Person search	**Threat items addressed** / **Throughput considerations** / **Staffing considerations**		
Manual person search	Has the potential to detect any threat items – procedure and thoroughness can be tailored to the threat items; Throughput depends primarily on the thoroughness required; easily scalable to match varying demand; Staff intensive but limited training required; physically demanding; best practice for manual screeners to be the same gender as the person being searched – need to ensure that the workforce has the correct gender balance	▶	**Example applications** • High demand, temporary deployments, with limited bags/possessions and where the focus is on larger threat items – low risk, space and frequency do not warrant use of technology • Very low demand, higher risk deployments with limited bags/belongings – space and/or limited demand preclude use of technology	**Example applications** • Low demand, higher risk deployments with larger/more complex bags/possessions ***NOTE*** *This is a relatively unusual combination.*
WTMD with HHMD resolution	Addresses only metallic threat items; sensitivity settings can be matched to the threat item; Throughput depends on the efficiency and effectiveness of the divest process, WTMD sensitivity settings, and the proportion requiring HHMD resolution; Regular training and good supervision required to ensure effective HHMD operation; good practice for HHMD operators to be the same gender as the person being screened	▶	**Example applications** • High demand, with limited bags/possessions, and where the focus is on larger/metallic threat items – low risk does not warrant the use of X-ray screening	**Example applications** • High demand, with larger/more complex bags/possessions, and where the focus is on larger/metallic threat items
WTMD with full manual search following an alarm	WTMD addresses metallic threat items; manual search covers both metallic and non-metallic threat items ***NOTE*** *Many WTMDs offer the option of random alarms to trigger additional manual searches.*; Throughput depends on the efficiency and effectiveness of the divest process, WTMD sensitivity settings, and the proportion requiring manual search; Manual person search is physically demanding; best practice for manual screeners to be the same gender as the person being searched – need to ensure that the workforce has the correct gender balance	▶	**Example applications** • Low demand, higher risk deployments with limited bags/possessions – space and/or limited demand preclude the use of X-ray screening	**Example applications** • Higher risk deployments with moderate to high demand and the need to screen larger/more complex bags/possessions; overall process required to provide a high level of assurance that threats will be detected

Key:

HHMD = hand-held metal detector

WTMD = walk-through metal detector

8 Implementation and deployment

8.1 General

Once the organization has formally stated its requirements for checkpoint security screening, it should address the following aspects of implementation and deployment:

a) general security measures (see **8.2**);
b) management and responsibility (see **8.3**);
c) operating procedures (including alarm resolution and response to the detection of threat items) (see **8.4**);
d) checkpoint location, design and layout (see **8.5**);
e) screening methods and equipment (see Clause **7**);
f) screening staff considerations (see **8.7**);
g) health and safety (see **8.8**);
h) security procedures (see **8.9**);
i) authority and consent to screening (see **8.10**);
j) privacy and ethical issues (see **8.11**);
k) training and maintenance (see **8.6** and **8.7.2**).

8.2 General physical security measures

a) The organization should ensure that the site perimeter is secure by including in its general physical security measures a physical perimeter (for example, robust fences, walls, windows, doors).
b) The organization should put in place systems and processes to manage entry and exit, based on an access control policy that considers all client groups.
c) The organization should put in place measures for detecting intruders (for example, alarm systems and CCTV supported by a guard response).
d) The organization should put in place any other measures deemed necessary.

The organization's risk assessment for the screening process should be very closely aligned with the overall security risk assessment. The operational requirement for the screening process should effectively be part of the operational requirement for perimeter security.

NOTE 1 *An insecure site perimeter means that any protection afforded by the implementation of a robust security screening process will be negated.*

NOTE 2 *For further information see advice on the Centre for the Protection of National Infrastructure's website: www.cpni.gov.uk/advice/Physical-security/.*

8.3 Management and responsibility

The organization's senior management should demonstrate commitment to all aspects of their organization's security including checkpoint security. There should be clear and appropriate management responsibility for checkpoint security and screening requirements and implementation, especially where this activity is contracted out. Management responsibility should be delegated to a named senior officer, who will be accountable for the correct operation of the organization's security procedures. The senior officer responsible for security should ensure that all staff understand the importance of good security practices, and are clear about their responsibilities. Management responsibility should be formally detailed in the operating procedures for checkpoint security screening.

Management should ensure that security measures are proportionate to the risk and that a balance is maintained between security and other organizational objectives.

The organization's management should regularly review checkpoint screening capability and security measures. Such reviews should include checks that screening processes are in accordance with the documented measures and address the operational requirement.

Whenever there is a material change to the organization or the threat, the organization should review the risk assessment for the whole of its security operations.

8.4 Operating procedures

8.4.1 General

The organization should have clear, formally recorded, operating procedures for checkpoint security screening.

When drawing up these procedures, the organization should assess how the level and type of screening may need to be changed depending on threat level (see **4.2.2**) and with variations in required throughput (see **5.2**).

The organization's operating procedures should address all client groups, as well as all relevant categories of vulnerable individuals (for example, minors) and those with other special needs. These procedures should describe, in detail, how each type of individual and their belongings are to be screened at the required level (see **6.2**).

The organization's operating procedures should describe the following:

a) which client groups and belongings are required to undergo which screening strategy (see Clause **6**) and under what circumstances (for example, everyone entering a particular location will be subjected to a full manual search). Where only a proportion of people are to be screened, a clear policy and process for selecting individuals should be defined;

b) detailed job descriptions, roles and responsibilities for screening staff, including details of standard deployment patterns and rotation between tasks within the screening process (or elsewhere);

c) detailed job descriptions, roles and responsibilities for those in the management hierarchy, especially team leaders and those responsible for the day-to-day management and operation of the screening process. Such roles will typically include responsibility for ensuring that equipment is maintained in a fully functional condition, and where necessary calibrated, and that the screening process is operating efficiently and effectively;

d) whether a witness should be present for all, or any parts of, the screening processes (for example, manual person searches, especially if conducted in private search areas), or screening of particular client groups (for example, minors or other vulnerable individuals);

e) measures (for example, daily checks) to ensure that screening areas are maintained in a safe condition, including ensuring that emergency exit routes are not obstructed, the environment is free of trip-hazards, and electrical cabling and equipment is undamaged;

f) alarm resolution processes;

g) emergency procedures for responding to the detection of threat items;

h) details of how decision making should be escalated if a threat item is found;

i) how other incidents, such as attempts by individuals to breach the checkpoint or avoid screening, should be handled;

j) contingency plans in case of partial or total unavailability of the screening process, for example, as a result of power or equipment failure, staff shortage, or some external factor preventing the screening facility being accessed.

NOTE *General guidance on response to the detection of a threat item is provided in Annex C.*

The organization should ensure that the operating procedures are accessible to and understood by all relevant staff. These procedures should form the basis of initial and continuation training of screening staff.

8.4.2 Incident response

The organization should implement a process for recording all incidents involving the detection of threats and other security incidents at checkpoints. Such a process should involve sufficient information being collated in a timely manner about the incident and associated response so that the information can contribute both to the organization's understanding of the threat it faces, and to a review of screening requirements and capability.

The organization's operating procedures, including emergency procedures, should be consistent with wider security measures employed in the organization.

The organization should be aware of the local emergency services' response requirements.

All responses to a discovered threat item should be proportionate to the seriousness of that threat to a particular building or event. Small non-explosive threat items may be dealt with easily whereas the discovery of an explosive device should invoke emergency procedures (see Annex C).

8.4.3 Review

The organization should regularly review and update its procedures. The organization should set a defined frequency for such reviews.

In addition, the organization should review all its procedures following any material change to the organization, to the nature and volume of movements of the various client groups through the checkpoint, or to the wider threat context.

The organization should review the effectiveness of its operational procedures, including emergency procedures, following an incident. The risk assessment should also be reviewed.

The organization should consider, as part of its wider risk assessment and contingency plans, the impact of loss of partial or total availability of its checkpoint screening measures.

8.5 Checkpoint design considerations

8.5.1 General

The organization should design its checkpoints so that they can cope with peak demand without undue delays to the individuals being screened.

NOTE 1 *This can be accomplished by scaling the screening operation by increasing or decreasing staff resource and screening capacity to meet demand.*

NOTE 2 *Multiple screening lanes are often used at large public events and other large sites; lanes may be opened and closed to meet fluctuations in predicted and/or actual demand.*

NOTE 3 *As a point of reference, a typical aviation security checkpoint can screen 150 to 200 passengers per hour per lane. The checkpoints at the London 2012 Olympic and Paralympic Games were designed for and achieved a throughput of 350 persons per hour per lane.*

NOTE 4 *The throughput rate depends on the types of threat item being sought, the screening strategy and process used, and types of clothing (for example, coats) and size/number of bags and possessions searched.*

NOTE 5 *The acceptable amount of delay may vary from one organization to another and also between different client groups.*

The organization should design its checkpoints so that they have enough space to accommodate staff, screening equipment and people being screened and their possessions. The organization should ensure that there is sufficient space on the entry side of the screening process to accommodate any queues of clients waiting to be screened.

The organization should ensure that the access route by which clients approach the checkpoint (including gateways, entrances and queues) is not a bottleneck that leads to the screening resource being used inefficiently.

Where multiple lanes are operating in parallel, the organization should distribute clients to them evenly and effectively, so that all lanes are utilized as fully as possible.

The organization should ensure that the exit route from the screening area should have sufficient capacity that it does not become a bottleneck that impedes the throughput of the screening process, or worse causes degradation of effectiveness as congestion causes the screening process to become difficult to manage.

Given the costs (staff, equipment, space) associated with providing screening capacity to address short, sharp peaks in demand, the organization should consider means of managing such peaks, for example, by encouraging flexible working patterns for staff, or staggering arrival times of different client groups.

Checkpoint design should support the required screening strategies, for example, consideration should be given to different lanes for different client groups according to the risks they present the level of screening required.

The organization should consider the space and location required for a private search area and how individuals will be escorted to and from such areas.

The organization should design its checkpoints so that incident response procedures can be carried out safely and effectively.

The organization should consider what communication equipment is needed to support the operation of the screening process, both normally and in the event of an incident or emergency. The organization should have a documented plan for the use of communication equipment in an emergency.

NOTE 6 *Communication options may include the use of fixed or mobile telephones, two-way radios and public address systems.*

8.5.2 Space required for X-ray screening

A typical X-ray machine for bags has screening tunnel dimensions of approximately 0.6 m wide × 0.4 m high. The organization should ensure that rollers or conveyors and/or tables are placed at the input and output of the X-ray machine to provide clients with a space where they can prepare for passing through the checkpoint. The length of the input and output rollers should reflect the throughput needed, the amount of preparation and divestment that is expected of the people being screened, and the space available.

8.5.3 Separation between metal detectors and other objects

Metal detectors can function in the proximity of metal objects. However, the organization should ensure that WTMDs are located at a sufficient distance from moving metal objects to avoid spurious alarms. A WTMD cannot distinguish between a small metallic object moving close by (the intended application) and larger metallic objects, moving even only slightly, that are further away. The organization should follow the manufacturer's guidance regarding the installation of any WTMD.

Large metallic objects that could cause a problem include X-ray machines, doors, temporary flooring, escalators, tent-struts and vehicles. Whilst the necessary separation can vary for different models, a minimum of 50 cm separation between a WTMD and an X-ray machine is typical.

The WTMD and any neighbouring X-ray machine should be mounted on a sturdy floor. WTMDs should also be kept away from cabling and potential sources of electromagnetic interference.

When multiple WTMDs are used in close proximity to each other, care should be taken to ensure that they are installed and configured according to the manufacturer's instructions so as to prevent interference, which could generate false alarms (see **5.3**).

NOTE *It is especially important to consider all of the above factors when constructing a temporary checkpoint as the environment will typically be more challenging for WTMD operation than for permanent installations (see **5.3**).*

8.5.4 Space required for manual person search

In operations where a manual person search is used for primary search or resolution of alarms on the body, space should be provided within the checkpoint area to carry out the search.

NOTE *The typical space required for carrying out a manual person search is a 1.8 m × 1.8 m square. However, it has been observed operationally that this can be reduced to a 1.3 m × 1.3 m square in space-constrained applications, since people can "share space" to some extent. In addition, screeners are not usually engaged in searching all the time. This may allow scope for further reduction of space. Reduction below a 1.3 m × 1.3 m square can have the effect of impairing search effectiveness, and also making it harder for staff to keep track of individuals, increasing the risk of someone escaping a secondary screening process in the resulting confusion.*

8.6 Equipment ownership considerations

The organization should identify and implement suitable measures for the management of the equipment used in the checkpoint throughout its life cycle, including the following:

a) during the planning phase: before any equipment is installed, a site survey should be conducted by the equipment manufacturer and/or expert consultants;

b) installation and setting up:
   1) provision of power and other utility supplies;
   2) control of environmental temperature and humidity;

   NOTE 1 *For installation and operation of X-ray equipment attention is drawn to the Health and Safety Executive's Ionising Radiations Regulations 1999 [3].*

c) security of systems:
   1) physical security of equipment to prevent loss, damage or tampering;
   2) procedures to prevent unauthorized use;
   3) IT security considerations such as password management, networking, backup and restoration procedures;

d) health and safety: considerations for installation, operation and maintenance of equipment;

e) calibration: calibration requirements will vary for different types of equipment and for different operating environments. The organization should ensure that equipment calibration procedures meet its particular operational needs. Points to consider include:
   1) initial set up and calibration of equipment including sensitivity levels;
   2) regular calibration and performance checking procedures, such as daily use of standard test pieces by designated staff;

f) maintenance:
   1) arrangements for periodic planned or preventative maintenance;
   2) arrangements to deal with equipment failure and downtime during maintenance;

   NOTE 2 *Some manufacturers offer service contracts with a guaranteed response time for rectifying failed equipment. It is important to ensure that the response time reflects the needs of the organization. The need for, and cost of, a quick response should be balanced against other contingency options such as tolerating longer queues or reducing screening standards slightly.*

g) record keeping:
   1) equipment logbooks;
   2) maintenance and configuration records;

h) ionizing radiation: management of any radioactive sources and systems using ionizing radiation, consistent with regulatory requirements. For screening this is relevant for trace detection and X-ray technologies. When X-ray machines are installed or relocated the organization should inform the Health and Safety Executive. A radiation survey should be performed by an individual trained in radiation protection;

   NOTE 3 *Further guidance may be obtained from the Health and Safety Executive, Public Health England. Attention is drawn to the Ionising Radiation Regulations 1999 [3].*

i) consumables: arrangement for supply and stock control management (including storage, expiry date management and reordering of any consumable items required for screening);

j) end-of-life:
   1) arrangements for the safe disposal of equipment and consumables at the end of their useful life;
   2) compliance with regulatory requirements;
   3) security considerations for equipment disposal;

k) temporary checkpoints: arrangements for the safe and effective storage, transportation, installation and commissioning, and dismantling of equipment used in temporary checkpoints. In cases where equipment is hired on a temporary basis the organization should consider whether settings and records are deleted prior to return.

8.7 Screening staff considerations

8.7.1 General

The skills, vigilance and awareness of staff are crucial to the success of checkpoint security screening operations. This applies both to the operation of security screening equipment and to the general management of the screening process. Even when screening equipment with some automatic threat detection capability is deployed, competent trained staff should be used for alarm resolution and response to any incidents.

The organization should encourage the optimum performance of staff and should have a well-defined management and leadership structure with clear reporting lines in place to facilitate this. The organization should appoint trained and experienced team leaders to supervise the screening process.

Team leaders should not normally participate directly in the screening process. Instead they should manage it, focusing on ensuring that it is running both efficiently and effectively and that alarms and incidents are dealt with appropriately. The team leader should act as a line manager for the screening staff.

A team leader should typically supervise no more than 10 to 12 staff.

NOTE *For small-scale screening operations (for example, screening occasional visitors to a small building), it may not be practical to have a dedicated supervisor.*

Screening staff should undertake their duties systematically and actively manage the flow of people through the checkpoint, not allowing anyone or anything to circumvent part or all of the screening process.

The organization should ensure that:

a) all staff are suitably trained to undertake their duties diligently;

b) screening staff have clearly defined roles; and

c) there is a clear management chain understood by all staff.

8.7.2 Training

All staff employed in the operation and management of the checkpoint should:

a) be trained in the screening methods and equipment that are deployed;

b) be able to demonstrate awareness of the broad range of threat items they may encounter; and

c) be trained in emergency procedures for the response to incidents.

Staff training should emphasize the overall objectives of the security screening task and not simply cover the component parts of the task. Consideration should be given to implementing communications and conflict resolution training. This is especially important where clients may not expect or understand the rationale for the screening process, for example, at large events.

Staff should receive refresher training in all aspects of their role at appropriate intervals and as required in response to changes to the threat.

The organization should determine the appropriate level and frequency of training and rehearsal of emergency procedures and should adhere to this. An auditable record should be kept of training and exercising activity.

8.7.3 Licensing

NOTE *The Security Industry Authority (SIA) is an independent body, reporting to the Home Secretary, which regulates the private security industry according to the Private Security Industry Act 2001. Its responsibilities include licensing individuals undertaking designated activities within the private security industry. One such licensed activity is manned guarding, which includes door supervision and security guarding.*

Whilst the screening/searching of people and bags/possessions is not per se a licensable activity it is often carried out in pursuit of a guarding activity (which is specified in the legislation) and the SIA advises that all private industry authorized personnel carrying out searches of people, bags/possessions or vehicles should be licensed.

The licensing of individuals does not negate the responsibility of the employer to provide job specific training. For more information see: www.sia.homeoffice.gov.uk/Pages/licensing.aspx.

8.7.4 Staff motivation

NOTE *Motivated staff generally perform well. Staff who lack motivation may cut corners, potentially reducing the effectiveness of the checkpoint screening process.*

The organization should try to ensure that staff remain well motivated, encourage managers to avoid issuing conflicting demands and look out for signs of reduced motivation in staff. For example, unreasonable throughput targets with actual or implied penalties may encourage screeners to cut corners. Poor staff morale within screening teams can also be expected to have a negative impact on the efficiency and effectiveness of the organization's security processes.

8.7.5 Staff effectiveness

It is recognized that many security tasks are repetitive, but require high concentration and vigilance; staff effectiveness has been shown to fall if they focus on a single task for too long. Certain screening tasks, such as manual search of persons, can also be physically demanding. Checkpoint operating procedures should stipulate how frequently staff should be rotated between tasks, and when they should take breaks (see **7.2.3.1**).

NOTE 1 *In most circumstances, it is highly unlikely that a screener will ever encounter a significant threat item. Over time this may be detrimental to the effectiveness of the process.*

NOTE 2 *If X-ray screening is used, threat image projection (TIP* ***see 7.2.3.2****) can be a useful tool for maintaining operator vigilance, and/or monitoring performance and motivation.*

8.7.6 Ergonomic considerations

Ergonomic considerations apply both to checkpoint staff and to the individuals being screened. The organization should design its checkpoint workspace and procedures to take into account ergonomic considerations relevant to maximizing the efficiency and effectiveness of the screening process. This should include:

a) the handling and preparation of bags, space and surfaces for divesting outer clothing and objects;

b) space and surfaces for repacking bags and replacing divested items; and

c) space and procedures for manual search.

At least some of the lanes should have sufficient space to be able to accommodate wheelchairs and pushchairs. Typically, the WTMD is the narrowest point within the screening lane, though steps, doorway gates and queues can also hinder access.

Other important ergonomic factors that the organization should consider include:

a) lighting levels – should be sufficient to enable thorough inspection of people/items during searches;
b) temperature – should be a comfortable working temperature for staff;
c) X-ray machine workstation – should have an adjustable chair and monitor that should be shielded from bright sunlight;
d) work surfaces for bag search – should be a comfortable working height and sufficiently spacious to allow the operator to unpack and search the expected bags to the required standard.

8.8 Health and safety

The organization should carry out a comprehensive health and safety risk assessment for the checkpoint process, considering both staff and the individuals being screened.

The assessment should also consider emergency response procedures in case of incidents. The health and safety risk assessment should cover specific points such as the presence of sharp or other hazardous items in bags (see **7.2.3.1**) and operation of equipment (for example, manual handling of heavy items, and the potentially physically demanding nature of manual searches). This risk assessment should be regularly reviewed and updated as required in response to:

a) changes to the threat; or
b) significant material changes to the organization, screening procedures or equipment.

Health and safety is everyone's responsibility and the organization should encourage all staff to report any concerns they may have. Safety checks should be conducted at the start of each working day or shift; these should consider points such as:

a) checking for trip hazards and damage to equipment;
b) ensuring that emergency exit routes are unobstructed; and
c) ensuring that the workplace is otherwise free from unnecessary items.

Any damage to equipment that may have safety implications should be reported immediately.

NOTE 1 *It is good health and safety practice to keep the workplace free of unnecessary items.*

For temporary outdoor installations, electrical safety is a particularly important consideration. The organization should ensure that equipment is specified appropriately and that a competent person oversees its installation.

NOTE 2 *All equipment has health and safety implications and attention is drawn to the* Health and Safety at Work Act 1974 *[4]. In particular, the use of X-ray equipment for baggage screening, certain types of body scanners that use X-rays and some other types of equipment that incorporate sources of ionizing radiation are subject to the* Ionising Radiation Regulations 1999 *[3], published by the Health and Safety Executive. Further guidance can be found on the Public Health England's website: www.gov.uk/government/organisations/public-health-england.*

8.9 Security procedures

8.9.1 Checkpoint security procedures

Details of the checkpoint security procedures (risk assessment, requirements, screening strategy, operating procedures, performance monitoring) should only be disclosed to those who have been deemed, prior to disclosure, as needing to have access to the information in order to perform their official duties. Such details include the following:

a) specific details of the types of threat items that the checkpoint is designed to detect (size, shape, materials);
b) specific details of the security process, for example, selection rules for screening or schedules for security operations;
c) details of the detection performance of the equipment and procedures deployed (especially detection rates and identified capability gaps);
d) health and safety risk assessments: these should be widely accessible to enable compliance and should be written in a way that does not provide specific details about the operation's capabilities.

The organization should consider the security of the checkpoint itself. For example, staff access should be restricted when the checkpoint is not in use. The organization should ensure that equipment settings can only be altered by designated managers.

All information relating to the screening process and the capability it confers should be managed using the organization's overall process for handling sensitive information.

8.9.2 Personnel security

The organization should implement good personnel security practice for staff involved in the management and operation of security checkpoints. This should include pre-employment screening and ongoing consideration of security.

NOTE 1 *Maintaining a security culture, screening for insider threats, controlling and monitoring employee access to sites and information, and exit procedures when staff leave the organization, are all important elements.*

NOTE 2 *Good practice guidance on personnel security can be found on the website for the Centre for the Protection of National Infrastructure (CPNI): www.cpni.gov.uk.*

8.10 Authority and consent to screening

NOTE 1 *The police, court officials and staff at schools and further education institutions have the authority to search or screen individuals and their belongings in particular circumstances. This authority is defined in a number of Acts of Parliament ranging from the* Poaching Prevention Act 1862 *[5] to the* Terrorism Act 2000 (Remedial) Order 2011 *[6].*

Any authority used by the organization for security screening should be clearly set out in the organization's policies/procedures and communicated to and understood by all screening staff and managers.

NOTE 2 *In most situations, client consent is required for screening. A valuable approach is to state that people and their belongings can be subject to search as a condition of entry to a building, facility or event.*

Any such condition of entry should be clearly communicated, for example, through signage displayed at the entrance to the site/checkpoint, as a condition of employment (for staff), or a condition of ticket purchase (for events).

NOTE 3 *Although screening normally requires consent, it is usually also within the rights of an organization to refuse entry to an individual who refuses to agree to being screened.*

8.11 Privacy and ethical issues

Checkpoint security screening inevitably impacts on the privacy of individuals being screened. The organization should ensure that any security screening undertaken is proportionate to the threat faced by the organization. Using the risk assessment, it should be possible to demonstrate the security benefits gained from the checkpoint screening process towards mitigating those threats.

The organization should carry out a privacy impact assessment. This assessment should consider how the security screening process may impact on individual privacy and assess this against the risks to the organization and potential benefits to be gained from security screening.

The organization should record the results of this impact assessment and regularly review and update it as required in response to changes in equipment, processes and threat. The organization should consider whether adjustments and processes can be put in place to mitigate any impact on privacy.

An effective privacy policy should be put in place by the organization to protect people being screened. This policy should consider what information or data may be captured when an individual passes through the checkpoint and whether this may be reasonably considered to be personal data. Where personal data is collected during the screening process, the organization should put in place appropriate measures to ensure that these data are destroyed or managed in line with data protection requirements.

NOTE *Attention is drawn to the* Data Protection Act 1988 *[7].*

Where selection is part of the security screening process, the organization should put in place policies and processes to ensure that individuals should not be selected on the basis of personal characteristics (that is, on a basis that may constitute discrimination such as disability, gender, sexual orientation, age, race, religion).

9 Monitor effectiveness and review

9.1 General

The organization should monitor and review periodically the effectiveness of the checkpoint screening operation as one of the inputs to the reviews of operational procedures (see **8.3** and **8.4**). The results of this monitoring and review should be stored by the organization in line with its security policy.

Monitoring and reviews can take into account a number of different performance measures (see **9.2**). Techniques are available for both continuous (see **9.3**) and periodic (see **9.4**) performance measurement. The organization should provide refresher training to address any particular performance problems identified. Refresher training should also be provided periodically for all staff to maintain awareness of good practice and give updates on the threat types and risks that the organization faces (see **8.7.2**).

9.2 Performance measures

The organization should select an appropriate set of measures to assess the performance of its checkpoint operation. These can include the following:

a) threat item detection performance measures:
   1) probability of detection;
   2) false alarm rate;
b) throughput measures:
   1) persons screened per hour;
   2) bags/possessions screened per hour;
   3) average and peak queue time;
c) staff performance measures;
d) customer satisfaction measures.

NOTE 1 *Measures can be applied to individual elements of the checkpoint, such as to particular pieces of equipment or to the overall end-to-end process.*

NOTE 2 *For a piece of detection equipment, system or process where the performance can be adjusted (either by changing the sensitivity of equipment or, for example, by changing the time available for an operator to interpret an image), there is a trade-off between the probability of detection (Pd) and the false alarm rate (FAR). Ensure system settings are correct when assessing performance.*

NOTE 3 *The probability of detection and the false alarm rate of a checkpoint system are a complex function of the performance of the individual pieces of equipment used, the screening and alarm resolution processes, and the staff who operate the checkpoint.*

9.3 Continuous performance monitoring

The organization should have procedures in place for monitoring and reviewing the performance (both efficiency and effectiveness) of the screening process. This should be achieved through a combination of on-the-job monitoring through the management chain, and other more independent activities such as inspection, testing, assurance and audit.

TIP can be an effective technique for continuous performance monitoring of X-ray operators (see **7.2.3.2**). TIP performance data (probability of detection and miss) should be routinely collated and examined by the security manager for assurance purposes and to highlight any further training needed.

NOTE 1 *Other effective monitoring methods include spot checks and random periodic testing (see **9.4**).*

The organization should use throughput measures to assess whether or not a checkpoint is meeting its design specifications and to highlight any particular issues that require attention.

NOTE 2 *As an example, actual queuing time versus target queuing time can be used as a measure of effectiveness.*

9.4 Periodic performance testing

9.4.1 Covert testing

Covert testing can be employed to test the performance of the checkpoint operation. If the organization does employ covert testing, this should be designed and managed with care, for example to avoid operators knowing when attempts are being made to test the checkpoint and to avoid unintended consequences (panic in staff or general public) on detection of a test threat item.

The organization should take particular care to ensure the safety of staff and the general public during this testing.

Where real or realistic-looking threat items are used, a process for the safe and secure storage, handling, presentation and control of such items should be established. This should include the labelling of items as inert/simulant as appropriate.

9.4.2 Routine equipment testing

The organization should periodically use reference test objects to assess performance of all its screening equipment. In the case of X-ray machines, the test objects should contain features, such as narrow metal wires, which represent the smallest features that need to be detected.

The organization should use two test pieces for checking the calibration of a WTMD – one representing the smallest object (for example, small knife/gun) that should reliably be detected, and the other representing the largest object (for example, keys/coins) that should not be detected.

NOTE *Such an approach will ensure that the system is set sufficiently, but not excessively, sensitively.*

Annex A (informative)
Location of screening facilities

A.1 General

The location of a security checkpoint within a building should be carefully considered, with the aim of minimizing the impact of any malicious attack. In most cases, an explosive device is the type of threat object that has the greatest potential for destruction. Even if the highest security screening level is deployed there will always be a possibility that a determined attacker can detonate an explosive device inside or close to the checkpoint area. For this reason, checkpoints should be located and designed in such a way as to mitigate the effects of blast and fragmentation on staff, visitors and the building's structure. A properly located and designed checkpoint will also assist business continuity by minimizing the impact of an attack at the checkpoint.

The location of security checkpoints and blast mitigation measures should be incorporated at the design stage of any new building. There should also be consideration of the intended use of rooms adjacent to the checkpoint area and the value of assets (both human and material) contained therein. Any structural design should be conducted by a suitably qualified expert in blast effects and structural engineering. Suitably qualified engineers may be members of the Register of Security Engineers and Specialists (RSES) administered by the Institution of Civil Engineers (ICE) or will be able to demonstrate that they have similar levels of competence to those required for membership.

In the majority of cases, security checkpoints are installed retrospectively inside an existing building. In such situations blast protection features should also be retrofitted. In the first instance, advice on likely threats and protective measures should be sought from a local police counterterrorism security advisor (CTSA). Following this a suitably qualified engineer should be consulted for advice on how a specific building can be "hardened" against blast. Further useful information may be obtained from the Centre for the Protection of National Infrastructure (CPNI) and the National Counter Terrorism Security Office (NaCTSO). An informative summary of protective measures can be found in Home Office Publication 16/13, *Guidance on Mitigation of Internal Explosions in Foyers and Entrances*, Home Office, 2013 [2].

The destructive power of an explosion is manifested in a shock wave travelling at supersonic speed. This is combined with the ensuing pressure rise caused by rapidly expanding gases generated in the explosion. Explosions are often accompanied by a localized fireball. The blast wave has the potential to cause fatal and serious injuries as well as damage to surrounding objects and structures. Vibration effects may cause damage to sensitive electrical equipment.

Fragmentation may be produced from the explosive device itself and any objects it may contain such as nails, bolts and other shrapnel. This is referred to as primary fragmentation. These fragments can be propelled at high velocities to considerable distances. Surrounding objects, such as fixtures and fittings, can potentially be thrown by the force of the blast or may shatter, producing large numbers of high velocity fragments. Collectively these are referred to as secondary fragmentation. Both primary and secondary fragmentation pose a significant risk to any occupants in the vicinity.

The highest secondary fragmentation risk is that from glazing. Unless strengthened, glass fails catastrophically when subjected to blast, generating numerous sharp, high velocity fragments.

A.2 Location – general recommendations

Where there is a significant risk of attack by explosive device, security checkpoints should be in the following locations:

a) outside buildings where possible, unless a specialist assessment by a qualified blast consultant advises otherwise;

b) away from vehicle checkpoints, vehicle entry points or car parks. As a general rule pedestrian entry/search points should be located at least 25 m to 30 m away from these;

c) away from sources of additional hazards that may arise following the detonation of explosives (for example, overhead glazing, gas supplies, chemical stores);

d) away from areas where crowds and large queues are likely to build up;

e) away from the venue or building being protected. Ideally the venue and security search facility should be separated by a distance of 65 m. This distance may be reduced if a specialist assessment by a qualified blast consultant advises otherwise. A distance of 65 m is generally not available at existing sites. However, efforts should be made to maximize the distance between the venue and the security search facility as far as practicably possible;

f) away from valuable assets (both human and material);

g) away from secondary or emergency routes to and from the venue.

A.3 Mitigation measures

In order to mitigate the blast effects following the detonation of an explosive device the organization should take the following measures:

a) reduce the hazardous fragmentation from glazing. Ideally all glazing should use laminated glass. Float or plain annealed glass should be avoided. In cases where it is not possible to replace existing glazing the use of bomb blast net curtains and anti-shatter film should be deployed. For further information see Home Office Guidance Note 11-08, *Glazing Enhancement to Improve Blast Resistance* [8], Home Office Guidance Note 11A-08, *Use of Anti-Shatter Film and Bomb Blast Net Curtains* [9] and Home Office Guidance Note 11B-08, *Peel Adhesion Testing of Anti-Shatter Film* [10];

   ***NOTE** At the time of publication, the documents are under CPNI review.*

b) ensure that any fixtures or fittings in the vicinity of the checkpoint area are suitably and securely anchored;

c) minimize the number of exposed structural columns or incorporate a surround that gives a stand-off distance to the column. This can reduce the likelihood of an explosive device being placed in direct contact with the column;

d) adopt good housekeeping practices by ensuring that security checkpoint areas are kept clean and free of obstructions. This can facilitate the identification of suspicious objects;

e) make sure that litter bins are not located close to the checkpoint screening areas as these offer potential concealment sites for explosive devices;

f) install blast-rated doors and walls close to a checkpoint screening area;

g) consider the designation of invacuation areas to protect staff and visitors in the event of the discovery or detonation of an explosive device.

A.4 Temporary checkpoints

The preceding sections concern the location of permanent checkpoints in a building or venue. The same principles should be adopted when setting up temporary checkpoints, for example, at a large public event. For temporary installations it is recommended that a local CTSA should be consulted for advice on probable threats and protective measures. A suitably qualified engineer (potentially from the RSES) should be consulted to conduct a preliminary survey of the venue. From this survey and in accordance with the general recommendations of **A.2**, the optimum location of the required temporary checkpoint should be identified.

Annex B (informative) Relevant standards

NOTE The following (non-exhaustive) list of British, international and other standards may be relevant to the design and implementation of checkpoint security operations.

B.1 General risk management and security standards

BS 7858:2012, *Security screening of individuals employed in a security environment*

Synopsis: BS 7858 is a security standard that helps employers to screen security personnel before they employ them. It sets the standard for the security screening of staff in an environment where the safety of people, goods or property is essential.

BS EN 15602:2008, *Security service providers – Terminology*

Synopsis: Provides a lexicon of security terms. The PAS uses some of these terms and also terms that are in general use in the checkpoint security screening field. Note that BS EN 15602, *Security service providers – Terminology* uses the alternative meaning of security screening as the "process of checking history and background of employees and potential employees".

BS ISO 22301:2012, *Societal security – Business continuity management systems – Requirements*

Synopsis: BS ISO 22301 specifies the requirements for setting up and managing an effective business continuity management system (BCMS) for any organization, regardless of type or size. It replaces BS 25999 *Business continuity management*.

BS ISO 31000:2009, *Risk management – Principles and guidelines*

Synopsis: BS ISO 31000 is the international standard for risk management. By providing comprehensive principles and guidelines, this standard helps organizations with their risk analysis and risk assessments. Related standards include:

a) BS 31100:2011, *Risk management – Code of practice and guidance for the implementation of BS ISO 31000*;

b) BS EN 31010:2010, *Risk management – Risk assessment techniques*;

c) ISO GUIDE 73:2009, ed. 1. *Risk management – Vocabulary*.

BS EN 60529:1992, Specification for degrees of protection provided by enclosures (IP code)

Synopsis: This standard describes a system (IP codes) for specifying the protection provided by the enclosures of electrical equipment against access to hazardous parts, ingress of foreign bodies and against the harmful effects of ingress of water. The IP codes of screening equipment may be relevant in the design and implementation of checkpoint systems, for example, temporary deployments that may be exposed to the weather.

B.2 Security equipment standards

B.2.1 Metal detector standards

ASTM C1238-97(2012) Standard Guide for Installation of Walk-Through Metal Detectors

Synopsis: This guide is intended for use by the designers, evaluators, and users of walk-through metal detectors to be installed to screen persons entering or leaving a controlled access area. This guide is not meant to constrain design liberty but is to be used as a guide in the selection of location and installation of walk-through metal detectors.

ASTM F2401-04(2010) Standard Practice for Security Checkpoint Metal Detector Screening of Persons with Medical Devices

Synopsis: This document is intended to address the needs and concerns of persons with implanted active medical devices or active ambulatory medical devices, as well as passive implanted medical devices, while maintaining the integrity of the security checkpoint.

NIJ Standard – 0601.02 (2003) Walk-Through Metal Detectors

Synopsis: This US National Institute of Justice (NIJ) standard specifies the minimum performance requirements and testing methods for walk-through metal detectors used by law enforcement, corrections and security for the detection of metallic weapons or contraband carried on a person and/or concealed by a non-metal object. The standard is being revised based on research performed by the National Institute of Standards and Technology, Office of Law Enforcement Standards.

NIJ Standard 0602.02 (2003) Hand-held Metal Detectors

Synopsis: This standard specifies the minimum performance requirements and testing methods for hand-held metal detectors used by law enforcement, corrections and security for the detection of metallic weapons or contraband carried on a person and/or concealed by a non-metal object. The standard is being revised based on research performed by the National Institute of Standards and Technology, Law Enforcement Standards Office.

NIJ is in the process of revising performance standards for walk-through metal detectors and hand-held metal detectors. The following documents are available as formal drafts or are under development.

NIJ Standard 0601.03 (2011) DRAFT Walk-Through Metal Detector Standard for Public Safety

Synopsis: This document is a voluntary equipment standard using a performance-based approach to specify clearly a minimum level of performance for each characteristic that has been determined to be critical to the equipment's intended use. It provides for three classifications based on detection capability by size and electromagnetic characteristic of objects:

a) metal detector (MD) Class 1: Objects nominally the size of a handgun;
b) MD Class 2: Objects nominally the size of a paring knife;
c) MD Class 3: Objects representing items such as short sections of hacksaw blades, hand-held paint scraper blades, screwdriver bits and handcuff keys.

NIJ 0602-03 (2011) DRAFT Hand-Held Metal Detector Standard for Public Safety

Synopsis: A voluntary equipment standard using a performance-based approach to specify clearly a minimum level of performance for each characteristic that has been determined to be critical to the equipment's intended use. NIJ Standard-0602-03 provides for four classifications based on detection capability by size and electromagnetic characteristic of objects. Those classifications are:

a) MD Class 1: objects nominally the size of a handgun;
b) MD Class 2: objects nominally the size of a paring knife;
c) MD Class 3: objects representing items such as short sections of hacksaw blades, hand-held paint scraper blades, screwdriver bits and handcuff keys;
d) MD Class 4: objects representing items such as paper clips, metal pen clips, metal pen refills, disposable razor blades and hypodermic needles.

NIJ SAG-0601.03 UNDER DEVELOPMENT Public Safety Walk-Through Metal Detector Selection and Application Guide

Synopsis: This document provides guidance concerning the procurement, selection, care, maintenance, training and administrative considerations related to WTMDs. The primary audience for this guide includes operators/screeners, supervisors, managers and purchasers in the law enforcement, corrections, public safety, courts security and school safety communities.

NIJ SAG-0602.03 UNDER DEVELOPMENT Public Safety Hand-Held Metal Detector Selection and Application Guide

Synopsis: This document provides guidance concerning the procurement, selection, care, maintenance, training and administrative considerations related to HHMDs. The primary audience for this guide includes operators/screeners, supervisors, managers and purchasers in the law enforcement, corrections, public safety, courts security and school safety communities.

NILECJ 0601-00 (1974) NILECJ Standard for Walk-Through Metal Detectors for use in Weapons Detection

Synopsis: This US National Institute of Law Enforcement and Criminal Justice (NILECJ) standard establishes performance characteristics and test methods for WTMDs. It defines five security levels and the corresponding objects to be detected, as well as nuisance alarms from normal pocket objects and carried items that should not cause alarms. Although superseded by later versions (above), this standard is still quoted by most of the manufacturers of WTMDs in their product specifications.

B.3 X-ray standards

BS IEC 62463:2010, Radiation protection instrumentation – X-ray systems for the screening of persons for security and the carrying of illicit items

Synopsis: This document lays down standard requirements and also specifies general characteristics, general test procedures, radiation characteristics, electrical characteristics, environmental influences, mechanical characteristics, and safety requirements. It provides examples of acceptable methods in terms of dose to the whole or part of the body for each screening procedure and the time taken for each screening procedure.

BS IEC 62709, DRAFT Radiation protection instrumentation – Measuring the imaging performance of X-ray systems for security screening of humans

Synopsis: This draft International Standard applies to X-ray security screening systems used to detect objects carried on or within the body. It covers both backscatter and transmission imaging systems. The object of this standard is to provide standard methods of measuring and reporting imaging quality characteristics and establish minimum acceptable performance requirements. Such technical performance testing complements explicit threat-detection testing and evaluation.

ANSI N43.17-2009 Radiation Safety For Personnel Security Screening Systems Using X-ray or Gamma Radiation

Synopsis: This standard applies to security screening systems that use X-rays and are designed to screen people. Specifically, this standard applies to systems used to detect objects carried on the individual being exposed. The standard provides guidelines specific to the radiation safety aspects of the design and operation of these systems.

ASTM F792-08 Standard Practice for Evaluating the Imaging Performance of Security X-ray Systems

Synopsis: Applies to all X-ray based screening systems, with tunnel apertures up to 1 m wide × 1 m high, whether it is a conventional X-ray system or an explosives detection system (EDS) that provides a projection or projection/scatter image for an operator to interpret. This practice relies upon the use of a standard test object (ASTM X-ray Test Object) to determine the applicable performance levels of the systems.

IEEE N42.44-2008 Performance of checkpoint cabinet X-ray imaging security systems

Synopsis: This document establishes standards for the technical performance of cabinet X-ray imaging systems used for screening at security checkpoints and other inspection venues.

IEEE N42.47-2010 American National Standard for Measuring the Imaging Performance of X-ray and Gamma-ray Systems for Security Screening of Humans

Synopsis: This standard applies to security screening systems that utilize X-ray or gamma radiation and are used to inspect people who are not inside vehicles, containers, or enclosures. Specifically, this standard applies to systems used to detect objects carried on or within the body of the individual being exposed. The purpose of this standard is to provide standard methods of measuring and reporting imaging quality characteristics and establish minimum acceptable performance requirements.

IEEE/ANSI N42.45-2011 American National Standard for Evaluating the Image Quality of X-ray Computed Tomography (CT) Security-Screening Systems

Synopsis: Test methods and test articles for the evaluation of the image quality of CT security screening systems are provided. The quality of data for automated analysis is the primary concern. This standard does not address the system's ability to use its image data to automatically detect explosives or other threat materials, which is typically verified by an appropriate regulatory body.

B.4 Other detection method standards

BS 8517-2:2010, Security dogs – Code of practice for the use of detection dogs

Synopsis: This standard gives recommendations for the operational use of detection dogs by detection dog handlers when providing passive and proactive detection services, for example, for drugs, firearms, munitions, explosives. It covers administration, kennelling/husbandry, health and welfare of the dogs, equipment and clothing, training, operational requirements, transportation, sale and gift of dogs.

B.5 National Occupational Standards

There are a number of National Occupational Standards (NOS) (www.ukstandards.co.uk) relevant to checkpoint security screening. NOS are a free resource for employers and training providers. They cover the spectrum of different occupations within the security sector and describe the knowledge and skills required to perform work to the nationally agreed standard for each specialism. These standards are determined by experts in their chosen field. At least two organizations Skills for Security (www.skillsforsecurity.org.uk) and Skills for Justice (www.skillsforjustice.com) provide NOS relevant to security screening. The NOS take the form of lists of role description elements and required skills capabilities.

Two particularly relevant NOS follow.

SFJ CCF G6 Maintain security using screening equipment.

Synopsis: This NOS is about screening individuals and items including personal baggage, clothing and other containers using electronic, X-ray and other forms of scanning equipment. Staff should ensure that the equipment is set up and operating correctly, follow all the correct procedures for screening individuals and items and respond correctly when unauthorized items are discovered. These may include firearms, explosives, drugs, knives and other items considered a risk and/or a threat.

SFS EVS 8 Conduct searches of people and their property before entering an event.

Synopsis: This NOS sets out the skills, knowledge and understanding required by staff to promote public safety and safeguard commercial interests through search. It covers searching of people and belongings for unauthorized items and response to finding these items.

Annex C (informative)
Action upon discovery of a threat item (or a suspicious item that could be a threat item)

C.1 General

This Annex gives general guidance through a non-exhaustive list of actions that may form part of an emergency response procedure relating to the discovery of a threat item of relatively high impact such as an explosive device. Lower impact threat items (a small knife may be an example) should be dealt with through a proportionately lower level of response to that given here. Action to be taken in all cases should be documented in the response procedures (referred to in **8.4.2**).

Threat items may be concealed or carried upon a person or within any belongings. The presence of the threat items may be known or unknown to the person and the level of cooperation in surrendering the threat item may vary. Response procedures should reflect this and the organization should ensure that it has response procedures in place for all threat items and situations. During development of response procedures the organization should contact the police to establish any relevant legal powers that staff may discharge during the course of their duties, particularly with respect to any offences committed and maintaining public safety.

C.2 Avoid unnecessary handling of threat items

a) If possible, and only if it is safe to do so, the threat item should be carefully placed upon a designated cleared flat surface and its location noted.
b) Once placed the threat item should not be moved or disturbed.
c) The threat item should not be further investigated.

C.3 Maintain control of the threat item and situation

a) The identified carrier of the threat item and any other unauthorized individuals should not handle the threat item.
b) If possible, and only if it is safe to do so, the identified carrier of the threat item should be made available for interview by the police.
c) If it is not possible or safe to take possession of the threat item, note its location and continue to monitor in a safe fashion.
d) Further organization security procedures relating to the discovery of a high impact threat item should be immediately invoked to ensure security.

C.4 Move away from the area

a) The immediate area should be cleared to a safe distance determined by the threat item type and impact.
b) Adjacent rooms including those immediately above and below should be evacuated where appropriate.
c) Individuals should be prevented from approaching or accessing the cleared areas.

C.5 Communications

a) If an explosive device is believed to be present, mobile phones and two-way radios should not be used in the cleared area or within 15 m of the explosive device.
b) Communicate clearly with staff, visitors and, where relevant, the public during the incident.

C.6 Notify the police

a) The police should be notified and the incident reported. The nature of the threat item, location and situation are likely to be requested.
b) Staff and other witnesses should remain available to brief or assist the police and record their observations of the incident in writing and independently of one another.

Bibliography

Standards publications

PAS 97:2012, *A specification for mail screening and security*.

Perimeter Security Standardization (Final Workshop Report), Publication of the ANSI Homeland Security Standards Panel.

Other publications

[1] THE CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE (CPNI). *Protecting Against Terrorism*, 3rd edition. London: CPNI, 2010.

[2] THE HOME OFFICE. Home Office Publication 16/13, Guidance on Mitigation of Internal Explosions in Foyers and Entrances. London: Home Office, 2013.

[3] GREAT BRITAIN. Ionising Radiations Regulations 1999, Health and Safety Executive. London: The Stationery Office.

[4] GREAT BRITAIN. Health and Safety at Work Act 1974. London: The Stationery Office.

[5] GREAT BRITAIN. Poaching Prevention Act 1862. London: The Stationery Office.

[6] GREAT BRITAIN. Terrorism Act 2000 (Remedial) Order 2011. London: The Stationery Office.

[7] GREAT BRITAIN. Data Protection Act 1988. London: The Stationery Office.

[8] THE HOME OFFICE. Home Office Guidance Note 11-08, *Glazing Enhancement to Improve Blast Resistance*. London: Home Office, 2008.

[9] THE HOME OFFICE. Home Office Guidance Note 11A-08, *Use of Anti-Shatter Film and Bomb Blast Net Curtains*. London: Home Office, 2008.

[10] THE HOME OFFICE. Home Office Guidance Note 11B-08, *Peel Adhesion Testing of Anti-Shatter Film*. London: Home Office, 2008.

Further reading

GREAT BRITAIN. Human Rights Act 1998. London: The Stationery Office.

Websites

NOTE *At the time of writing many UK government websites are now accessible via www.gov.uk.*

Centre for the Protection of National Infrastructure (CPNI)
www.cpni.gov.uk

Department for Transport
www.dft.gov.uk

Health and Safety Executive
www.hse.gov.uk

The Home Office
www.homeoffice.gov.uk

The Institute of Risk Management
www.theirm.org

National Counter Terrorism Security Office (NaCTSO)
www.nactso.gov.uk

National Occupational Standards (NOS)
www.ukstandards.co.uk

The Police
www.police.uk

Public Health England
www.gov.uk/government/organisations/public-health-england

Register of Security Engineers and Specialists (RSES)
http://www.ice.org.uk/qualification-careers/Professional-Registers/UK-Professional-Registers/The-Register-of-Security-Engineers---Specialists

Security Industry Authority (SIA)
www.sia.homeoffice.gov.uk/Pages/licensing.aspx

Skills for Justice
www.skillsforjustice.com

Skills for Security
www.skillsforsecurity.org.uk

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similarly for PASs, please notify BSI Customer Services.

Tel: +44 (0)845 086 9001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)845 086 9001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website **www.bsigroup.com/shop**. In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)845 086 9001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)845 086 9001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at **http://shop.bsigroup.com/bsol**

Further information about British Standards is available on the BSI website at **www.bsigroup.com/standards**

Copyright

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com

ISBN 978-0-580-79006-5