PAS 97:2015

Mail screening and security – Specification

CPNI
Centre for the Protection
of National Infrastructure

bsi.

Publishing and copyright information

ISBN 978 0 580 89290 5

ICS 13.310

Publication history

First published March 2009
Second edition January 2012
Third (present) edition October 2015

Contents

Annexes

List of figures

List of tables

Foreword

This Publicly Available Specification (PAS) was sponsored by the Centre for the Protection of National Infrastructure (CPNI). Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution (BSI). It came into effect on 31 October 2015.

Acknowledgement is given to the following organizations that were involved in the development of this PAS as members of the steering group:

- Atkins Ltd
- Bank of England
- Centre for the Protection of National Infrastructure (CPNI)
- Credit Suisse
- Department for Communities and Local Government
- Department for Education
- Metropolitan Police Service
- PosteRoute Ltd
- Royal Mail
- Sellafield Ltd
- Sister Banks Group
- Swiss Post Solutions Ltd
- UK Parliament

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

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

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a specification to be rapidly developed in order to fulfil an immediate need in industry. A PAS can 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.

Supersession

This PAS supersedes PAS 97:2012, which is withdrawn.

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

In this PAS, the word "shall" indicates requirements. The word "should" is used to express recommendations of this standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event. All wording without use of these verbs is general commentary that provides a framework for useful understanding of the provisions of this standard. Paragraphs marked "NOTE" offer particular guidance in understanding or clarifying the associated requirement.

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 a PAS cannot confer immunity from legal obligations.

Introduction

Even in this electronic age, most businesses and other organizations rely on the ability to receive and send physical items of mail. As an essential part of normal operations, mail presents various potentially significant vulnerabilities. Mail streams into and within an organization provide a vector for malicious attacks and scope for other security incidents, all of which can adversely affect the day-to-day business of the organization, as well as its reputation.

Attacks might be intended to cause physical damage to property, harm to individuals, to create fear or merely to cause disruption. Conversely, it is also quite possible for perfectly benign objects to appear suspicious, causing disruption through emergency responses that prove unnecessary. In addition, incoming and outgoing mail streams might contain valuable items or sensitive information that warrant protecting from loss or theft.

Mail screening and security measures can be used to reduce the risk and impact of such incidents. This PAS aims to assist organizations in identifying and implementing appropriate postal security measures that meet their particular needs.

Too few or inappropriate measures increase the risk of significant security incidents that harm the organization and its business. Excessive measures are likely to be an unnecessary expense and might otherwise reduce the efficiency of the organization, for example by causing delays or using scarce staff and space resources.

In working to identify and implement the appropriate measures for an organization, it is important to consider factors both within and external to the organization as well as potential future changes to these. For example, the nature of the organization's business could change in a way that affects mail throughput requirements, as could the public profile of the organization in a way that makes it more likely to be targeted by single-issue groups, terrorists or disaffected individuals.

Case Study A – US Anthrax Letters, 2001

In September and October 2001, letters containing *Bacillus anthracis* spores were mailed to several news media offices and two US Democrat Senators. Five people died of inhalational anthrax and more than a dozen others became seriously ill. Thousands of employees of the US Postal Service and government offices that could have been exposed were given antibiotics as a precaution. Dozens of buildings were contaminated as a result of the mailings. The attack had a severe impact on mail services across the United States as many postal facilities had to close for decontamination. One building took three years to reopen after decontamination at a cost of many tens of millions of dollars.

US Federal prosecutors eventually declared a scientist employed in the government's bio-defence laboratories as the sole perpetrator, though his motives for the attacks were unclear.

Case Study B – UK Letter Bomb Campaign, 2007

In January and February 2007, there was a targeted mail campaign in the UK against seven companies and government agencies which the perpetrator believed were connected to a rise in a "surveillance society". Relatively unsophisticated explosive devices were used, most of which functioned on opening causing minor injuries to the hands and upper bodies of the persons handling the items and other persons nearby. Due to the different ways in which organizations handle incoming mail, those who opened the letters and were injured were not necessarily the intended targets for the devices. In two cases the items were intercepted by trained and vigilant mail room operators and dealt with safely using practised escalation procedures, resulting in minimum disruption to the organizations concerned.

In September 2007, Miles Cooper, a school caretaker from Cambridge, was found guilty of a variety of charges in relation to the letter bomb campaign, and received an indeterminate prison sentence.

Case Study C – UK Hoax Campaign, 2012

A series of hoax "anthrax" letters were sent to high profile government officials, including the Deputy Prime Minister, in the summer and autumn of 2012. The letters were intercepted at a mail screening centre, and the substance found to be non-hazardous. If the letters had not been intercepted the campaign would undoubtedly have caused concern and disruption.

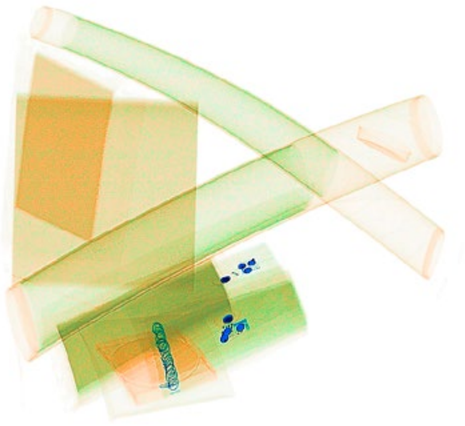
Ruth Augustus was found guilty of six counts of hoaxes involving noxious substances and was sentenced to a two-year community order in addition to receiving mental health treatment.

Case Study D – US Ricin Letters, 2013

On 16 April 2013, an envelope addressed to a US Senator was intercepted at the US Capitol's offsite mail facility in Washington DC and tested positive for ricin. The following day a second envelope, this time addressed to the President of the United States, was intercepted and again tested positive for ricin. A further letter containing ricin reached its intended recipient, however the individual was not harmed.

Everett Dutschke was charged in June 2013 for developing and possessing ricin toxin and subsequently mailing ricin-laced, threatening letters, including one that threatened bodily harm to the President of the United States. He was sentenced to 25 years in prison.

The events sparked numerous copycat incidents with individuals mailing ricin to a senior judge and the Mayor of New York.

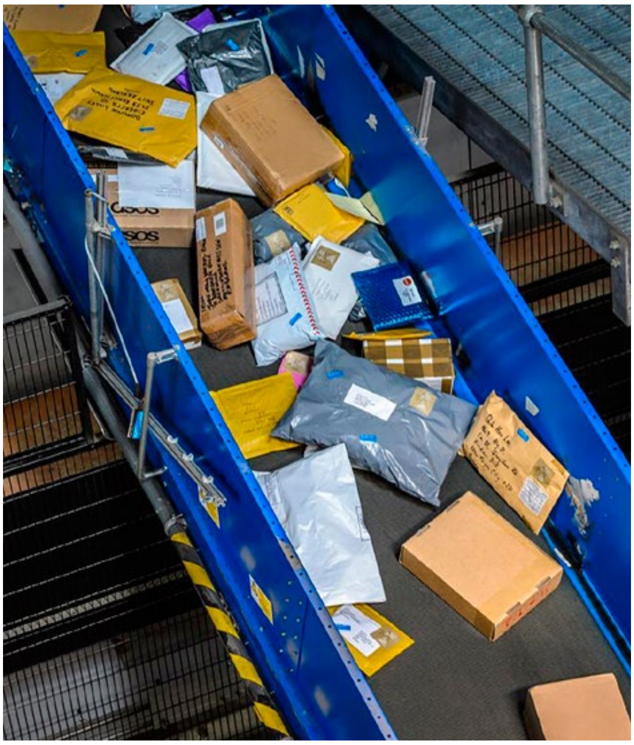


Case Study E – UK Parcel Bombs, 2014

In February 2014 a series of parcel bombs were sent to several British Armed Forces Careers Offices across England. All the devices were contained within envelopes which were addressed by hand. A group linked to Northern Irish terrorism claimed responsibility for the packages in a statement made to the Irish News. If they had not been discovered, the crude but potentially viable devices were likely to have caused harm to their victims.

Case Study F – Mail Screening Requirements of the Offshore Oil and Gas Industry

Whilst security is an important issue for the oil and gas industry, safety is paramount; hence alcohol and drugs are prohibited on all offshore oil and gas installations. Employees and contractors are required to declare all medical conditions and any drugs prescribed to them to treat these conditions. Mail to offshore installations is routed internally within the respective organization – it is received at a company office on land where it is screened for alcohol and drugs (both prescribed and illegal), as well as hazardous materials and items, before being transferred offshore.



1 Scope

This PAS specifies requirements and gives recommendations for mail screening, set in the broader context of postal security. It is intended for use by those responsible for planning, delivering or procuring mail handling and screening services within organizations, as well as commercial providers of such services.

It specifies measures to assist businesses and other organizations in identifying and minimizing the impact of items of mail that represent a threat, or could otherwise cause concern or disruption. It also addresses broader postal security measures aimed at ensuring all incoming, outgoing and internal mail streams are managed so as to minimize the risk of loss or theft of valuable or sensitive items or information.

This PAS concentrates on letters and small parcels entering the organization from any external source, including public/commercial postal services, by hand or by courier delivery.

Whilst many of the principles detailed in the PAS can also be applied to improving the security of other, larger-scale deliveries, these are not explicitly covered.

The security of electronic mail and associated IT systems is outside the scope of this PAS.

This PAS does not propose a single standard of postal security and screening. Instead, it sets out to assist organizations in assessing their particular level(s) of risk, and selecting and implementing commensurate security measures whether onsite or offsite, delivered in-house or outsourced. A series of screening levels (1 to 5) is defined in terms of progressively more complex screening measures; this is complemented by a series of physical protection classes (A to D) that describe incremental physical protective measures for mail rooms and personnel.

***NOTE** Another factor contributing to the overall level of protection an organization derives from its postal security measures is the location of its mail facilities.*

2 Terms and definitions

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

2.1 deliveries

goods received by an organization

***NOTE** This includes mail and a broad range of other, often larger, items (for example cleaning, catering and office supplies and equipment) which present different challenges.*

2.2 mail

letters and small packages, which could be delivered by a commercial postal operator or courier company, be hand delivered or originate within the organization

***NOTE** Whilst "post" and "mail" are commonly used interchangeably, the term "mail" is used throughout this PAS (with "postal" used as the corresponding adjective).*

2.3 mail handling

all aspects of moving mail **(2.2)** around within an organization, including collection, sorting, distribution and delivery

2.4 mail room

room or multi-room facility where mail **(2.2)** is sorted and/or screened

2.5 mail screening

use of manual or automated methods to identify hazards and other causes of disruption associated with items of mail **(2.2)**

2.6 mail streams

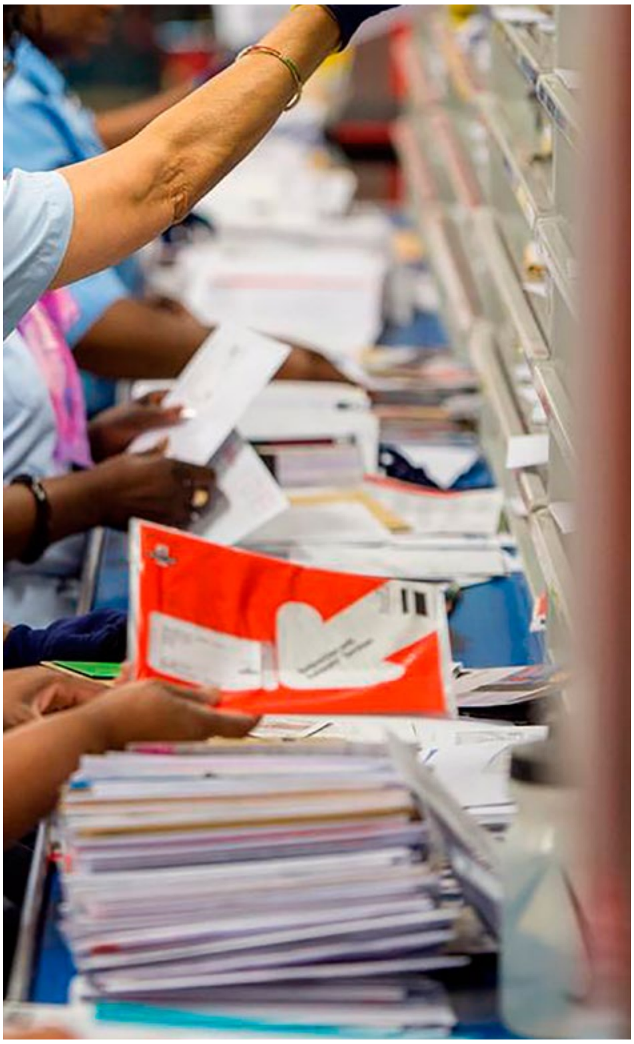
routes by which mail **(2.2)** travels from sender to recipient

*NOTE 1 Most relevant in the context of this PAS are streams within the organization in question, i.e. how mail **(2.2)** enters, travels within, and exits the organization.*

*NOTE 2 Mail streams within the organization may span multiple sites or include offsite mail handling **(2.3)**/ screening **(2.5)** by specialist contractors.*

2.7 personnel security

system of policies and procedures which seek to manage the risk of staff (permanent, temporary or contract staff) exploiting, or intending to exploit, their legitimate access to an organization's assets or premises for unauthorized purposes



2.8 postal security

encompasses both mail screening **(2.5)** and more general measures aimed at making sure all incoming, outgoing and internal mail streams **(2.6)** are managed so as to minimize risk **(2.9)**

2.9 risk

reflects the impact and likelihood of an incident arising as a result of the threat **(2.12)**

2.10 sensitive information

information that may warrant protecting (including while in transit in mail **(2.2)**

NOTE This may include intellectual property, trade secrets or confidential personal, financial or medical information.

2.11 specialist (security) engineers

engineers who are members of the Register of Security Engineers and Specialists (RSES) or are able to demonstrate competencies similar to those required for RSES membership (see Bibliography for information on the Register of Security Engineers and Specialists)

2.12 threat

the ways in which, and reasons why, an organization may be targeted

2.13 "white powders"

encompasses hazardous chemical (including explosive or narcotic), biological or radiological materials, as well as benign materials

NOTE Such materials may not be "white" and may not be "powders"; materials may be crystalline (e.g. sugar), oily or waxy residues, or liquids.

3 Outline of process

The organization (including its appointed contractors where appropriate) shall assess the risks associated with postal incidents (see Clause **4**). This assessment shall require consideration of the threats the organization faces (see **4.2**) and of the vulnerability of its mail streams and associated processes, and the potential impact of mail-related incidents (see **4.3**).

The organization shall aim to reduce, to an acceptable level, the risk of postal incidents causing disruption or harm.

NOTE 1 *An acceptable level of risk is the level of residual risk the organization is prepared to accept.*

The organization shall identify an appropriate level (or levels) of screening (see Clause **5**) combined with suitable physical protective measures (see Clause **6**). The organization shall record the findings of this analysis, formally stating its requirements (see Clause **7**), and then shall implement these measures accordingly, with regular review (see Clause **8**). The overall PAS 97 process is summarized in Figure 1.

The organization shall follow all of the steps described in this PAS, and shall consider postal security as an integral part of its wider security measures.

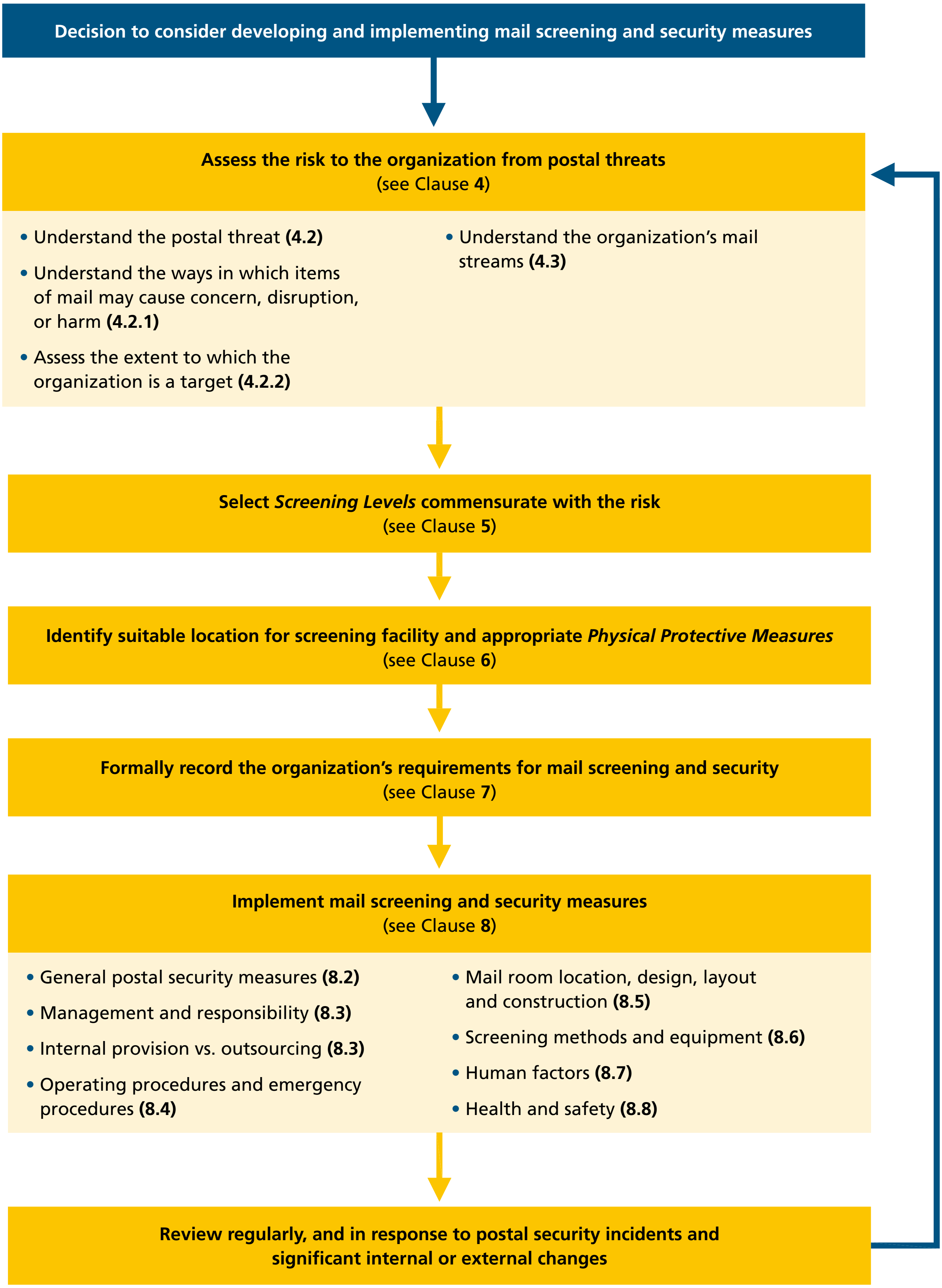
WARNING Ad hoc adoption of individual measures described in this PAS could lead to the implementation of an inadequate screening capability, or to unsafe practices. For example, selecting a particular level of screening without also using an appropriate class of physical protection measures could result in staff being unnecessarily exposed to hazards.

NOTE 2 *More general information on business risk management can be found in BS 31100, Risk management – Code of practice and BS EN ISO 22301, Societal security – Business continuity management systems – Requirements, as well as from the sources in the Bibliography. More general information on security management can be found in BS 16000, Security Management – Strategic and operational guidelines.*

Organizations demonstrating or requesting compliance with measures set out in this PAS shall do so using the format “PAS 97:2015 at Screening Level n with Physical Protection Class x”.

NOTE 3 *When demonstrating or requesting compliance, supplementary information (for example exceptions, additional measures or details of location) should be supplied as required.*

Figure 1 – Summary of PAS 97 process



Decision to consider developing and implementing mail screening and security measures

Assess the risk to the organization from postal threats
(see Clause **4**)

- Understand the postal threat **(4.2)**
- Understand the ways in which items of mail may cause concern, disruption, or harm **(4.2.1)**
- Assess the extent to which the organization is a target **(4.2.2)**
- Understand the organization's mail streams **(4.3)**

Select *Screening Levels* commensurate with the risk
(see Clause **5**)

Identify suitable location for screening facility and appropriate *Physical Protective Measures*
(see Clause **6**)

Formally record the organization's requirements for mail screening and security
(see Clause **7**)

Implement mail screening and security measures
(see Clause **8**)

- General postal security measures **(8.2)**
- Management and responsibility **(8.3)**
- Internal provision vs. outsourcing **(8.3)**
- Operating procedures and emergency procedures **(8.4)**
- Mail room location, design, layout and construction **(8.5)**
- Screening methods and equipment **(8.6)**
- Human factors **(8.7)**
- Health and safety **(8.8)**

Review regularly, and in response to postal security incidents and significant internal or external changes

4 Assessing the risk

4.1 General

The first step in identifying and implementing appropriate mail screening and security measures involves understanding the risks associated with each of the various mail streams into and within the organization. This requires consideration of current and possible future threats to the organization and the likelihood and impact of an incident occurring.

NOTE *Further measures for business continuity can be found in BS EN ISO 22301, Societal security – Business continuity management systems – Requirements.*

4.2 Understanding the threat

4.2.1 Mail causing concern, disruption or harm

4.2.1.1 General

Those responsible for postal security within an organization shall have a clear understanding of the ways in which items of mail could cause concern, disruption or harm, either unintentionally or as a result of malicious intent.

An individual might pursue an attack on an organization through the mail because it is a targeted, "anonymous" approach, which offers a direct route into the organization and has the potential to cause significant impact.

NOTE 1 *An unopened postal item may raise concerns on account of its external appearance. It may be benign but of unusual appearance or it may be intended to cause concern, disruption or harm, either as a hoax or an obvious hazard. Alternatively, an item of mail may be intended to cause harm or disruption but without its external appearance raising particular concerns. A more involved process, i.e. at one of the higher screening levels set out in Clause* ***5****, is necessary to detect this kind of threat. A list of possible indicators that a delivered item may be of concern is presented in Annex A. This list is quite general, and what may be deemed suspicious in one context may be quite normal in another.*

From a screening perspective, it is helpful to consider hazardous items and materials as falling into two categories:

a) discrete threat objects and bulk materials;

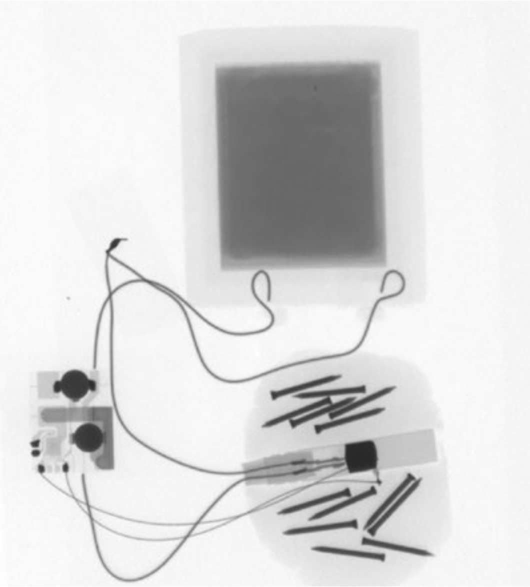
b) "white powders" (see **2.13**).

NOTE 2 *Disruption or concern may be caused by hoaxes intended to look like such threat objects and materials. The sending of hoaxes is a criminal offence; suspected hoax incidents should be reported to the police.*

NOTE 3 *Disruption or concern may also be caused by offensive written or graphical material, either within or on the outside of the item of mail; whilst in itself physically harmless, it may be distressing to the recipient, and importantly it may also be indicative of the presence of other hazards. The sending of offensive written or graphical material is a criminal offence; incidents should be reported to the police.*

4.2.1.2 Discrete threat objects and bulk materials

This covers items and bulk quantities of hazardous materials whose presence should be clearly discernible when mail is X-rayed, even if a large volume of mail is X-rayed at once.



This category includes:

- explosive and incendiary devices (improvised or of commercial or military origin);
- firearms and ammunition;
- knives;
- blades and other sharp items, (e.g. syringe needles, broken glass);
- offensive material (e.g. faeces, urine);
- bulk chemicals – toxic, corrosive or otherwise harmful, including narcotics;
- bulk biological materials;
- bulk radiological (radioactive) materials.

Relatively straightforward, high-throughput X-ray screening can offer a very good level of protection against discrete threat objects and bulk materials. If such a threat is present it is likely to be discernible in the X-ray image, provided the image is not too cluttered and the operator is suitably trained, experienced and alert. Repeat X-raying of smaller batches or individual items can help resolve items in cluttered images.

4.2.1.3 "White powders"

This covers smaller amounts of chemical, biological or radiological materials that are unlikely to be readily discernible when items of mail are X-rayed, especially when X-rayed in bulk. These materials may be dispersed within envelopes or packages (so have no obvious shape, unless aggregated in a corner as a result of gentle tapping or transit through the postal system); be fundamentally poor at absorbing X-rays; and/or be present in sufficiently small quantities as to be effectively invisible when X-rayed.

NOTE *People often refer to "white powders" in the context of postal threats. These can include hazardous chemical (including explosive or narcotic), biological or radiological materials, as well as benign materials. It is important also to note that such materials may not be "white" and may not be "powders"; materials may be crystalline (e.g. sugar), oily or waxy residues, or liquids.*

Bulk X-ray screening offers very limited protection against "white powders" and there is no other simple high-throughput technical solution offering the required breadth of screening capability. Increased certainty of detection can only be derived from increased manual effort.

4.2.2 To what extent is the organization a target?

The organization shall assess the extent to which, and the reasons why, it could be a target. This assessment shall take account of the fact that the organization is unlikely to be homogeneous, and it and the context in which it operates are unlikely to be static. Different parts of the organization could be targeted to different extents and for different reasons. The assessment shall therefore consider the organization as a whole and also as its constituent parts (divisions, brands, departments, sites, buildings, etc.).

The assessment shall also consider whether, and the reasons why, specific individuals might be targeted. Consideration shall be given to senior executives and any other staff with a public profile, as well as to managers in areas where there is potential for employees to be particularly disgruntled.

NOTE 1 *Official threat levels published by the government are necessarily general in their nature. As such they could inform, but are no substitute for, the organization's own detailed assessment of the threats it faces.*

Consideration shall be given to what elements of its business might, in the widest sense, be perceived as attractive targets.

NOTE 2 *This assessment should include things the organization itself does or stands for, including sponsorship relationships; things other organizations in the same industry might do or stand for; as well as links through the supply chain to other organizations, quite possibly in different industries. High profile individual members of the organization, especially those who publicly express views on potentially contentious matters, should also be considered.*

The assessment shall also examine how and why the organization might be targeted internally, for example by potentially disgruntled employees or groups of employees, such as those facing or fearing redundancy.

Use of multi-occupancy buildings (and to a lesser extent, sites) can have associated risks as the targeting of other occupant organizations is likely to have an impact, especially if mail room facilities are shared; such factors shall be included in the threat assessment.

Consideration shall be given to the range of ways in which the risk to the organization might change over time.

NOTE 3 *Changes to the organization's business (e.g. through development, merger or acquisition) might lead to it becoming more of a target, as might appointment of a high profile individual; widespread or localized deterioration of relations with staff could likewise increase the risk. There are also wider external factors over which the organization might have little control* *such as changing public opinion over the nature of the organization's business, as well as evolving terrorist threats.*

The threat assessment shall be reviewed regularly, and additionally in the event that there is a material change within, or external to, the organization.

4.3 Understanding the organization's mail streams

4.3.1 Assessing vulnerability to and impact of suspicious or hazardous mail

As part of its overall risk assessment process, the organization shall identify and understand all incoming and internal mail streams. This analysis shall consider all possible addresses for the organization, i.e. all the organization's sites, as well as any PO Box addresses. For each mail stream, both the likelihood and impact of an incident shall be considered, with this analysis informing decisions about levels of screening and associated protective measures.

Mail streams into the organization (or site or building) typically include:

- deliveries by public or commercial mail services;
- courier deliveries;
- items hand delivered to entrances/receptions, etc.;
- internal mail, e.g. from other sites.

NOTE 1 Some of these streams might warrant being subdivided for the purposes of this analysis. For example, items addressed to high profile individuals (by name or by position) or specific flagship addresses could be particularly likely to be targeted.

The analysis shall be sufficiently thorough as to identify any minor and less obvious routes by which mail could enter the organization, so that efforts can be made to ensure that these streams, which might present particular threats, do not circumvent any screening measures, either inadvertently or intentionally.

NOTE 2 "Urgent" or "important" items, especially those delivered out of hours, and hand delivered items for "VIPs" within the organization, are particularly good examples of such streams.

NOTE 3 There is a risk that staff might encourage correspondents to send mail to unscreened addresses (e.g. home addresses), either for reasons of expediency or specifically to circumvent security measures. Use of such addresses should be carefully monitored; such addresses should never be announced publicly.

The organization shall consider the implications of staff receiving personal mail and other items (e.g. mail order and internet shopping deliveries) at work. Whilst a simple solution is to prohibit such deliveries, this might not be practical or acceptable. All personal deliveries shall therefore be subject to the appropriate level of screening. The organization shall consider the legal implications of screening personal deliveries, including privacy issues and the risk of accidental damage to the contents, and inform staff accordingly.

Generally, internal mail streams within an organization will present a relatively low risk provided their integrity is not compromised through poor security during storage and transit. In contrast, unexpected courier and hand delivered items might represent a particularly high risk, whilst the risk is probably much lower for specific items from trusted contacts whose delivery is expected. Mail to some high profile, widely known individuals or addresses might represent a higher risk than mail to other, lesser known individuals or addresses.

NOTE 4 "VIPs" (and their personal assistants) can believe that they are "above" security processes and hence try to circumvent them.

The organization shall understand how an incident might affect its business, noting that disruption to different mail streams could impact it in different ways.

NOTE 5 For example, emergency measures implemented in response to an incident might physically prevent access to, or use of, parts of a building, but might also lead to delays in delivery of mail to otherwise unaffected areas. Mail streams to specific functions within an organization might be particularly critical to its business, and hence justify extra screening or priority handling.

Having carried out this analysis, the organization shall consider whether the risk from postal threats can be reduced in any other ways before committing to specific screening measures.

NOTE 6 An example of such an approach would be rerouting mail streams away from particularly vulnerable areas.

4.3.2 Valuable items and sensitive information

Most organizations need to safeguard valuable items and sensitive information against loss or theft.

The organization shall identify the sorts of valuable items and sensitive information that might be transported within its mail stream, taking a broad view of what could be valuable or sensitive and hence potentially damaging if lost or made vulnerable to theft.

Combining this information with the previous analysis of its mail streams, the organization shall consider the relative importance of protecting its various incoming, internal and outgoing mail streams.

5 Screening levels

5.1 General

Generally, the greater the commitment of resource and effort to mail screening, the greater the protection that is likely to be achieved. It is, however, important that the organization achieves an appropriate level of screening, balancing the threat it faces with the need for operational efficiency. Additionally, the organization shall have the flexibility to adapt screening in response to changes to the threat or the requirements of the organization's business.

It might be appropriate to apply different levels of screening to different mail streams, to reflect the different risks associated with the various streams. For example, internal mail normally represents a relatively low risk, while unexpected hand delivered items and mail addressed to high-profile individuals might warrant particularly high levels of screening.

Similarly, stamped mail, which is most likely to be from individuals or small organizations, could be seen as representing a higher threat than franked mail from larger organizations.

5.2 Selecting appropriate screening levels for different mail streams

Before selecting appropriate screening levels, the organization shall understand the risks to its business from postal incidents. Threat and impact assessments shall have been carried out, and all mail streams shall have been identified and understood, with relative risks ascribed to each stream.

The organization shall decide and record which screening level is applied to each of its various mail streams in accordance with Table 1, and implement the appropriate measures robustly and with regular review. As part of this process, the organization shall also consider potential future requirements that might arise from changes to the threat climate or changes to mail streams.

NOTE 1 *The higher the screening level, the more involved and resource intensive the process is: space, equipment and staff (including training) requirements are likely to be greater. If there is little or no flexibility in the available resource, a higher screening level will result in a lower throughput. It is therefore important to consider the wider implications of selecting a high screening level or raising the screening level, for example, as a result of a change to the threat.*

Such implications might include delays in the screening and release of mail, which might adversely affect other aspects of the organization's business.

NOTE 2 *Official threat levels published by the government are necessarily general in their nature. As such they could inform, but are no substitute for, the organization's own detailed assessment of the threats and risks it faces. For this reason the screening levels in Table 1 are not directly linked to the official threat level scale.*

NOTE 3 *There is a wide variety of specific screening technologies available that only offer capability against a small proportion of the overall spectrum of potential threat materials and items. Whilst such threat-specific screening approaches might be appropriate for some organizations (and/or mail streams) in some circumstances, they can leave the organization particularly exposed to sudden changes in the nature of the threat. Decisions surrounding the selection and implementation of specific technologies are therefore particularly complex. For these reasons, the screening levels set out in this PAS focus on technologies (e.g. X-ray screening) and approaches (e.g. visual inspection) that maximize the capability to detect a broad range of threat materials and items.*

Table 1 – Screening levels

Level	Screening method	Protection afforded against		Measures common to all screening levels
		Discrete threat objects and bulk materials	"White powders"	
(0)	No screening, other than general staff awareness of postal threats	Low	Very low	The chosen screening level(s) shall be implemented in combination with physical protective measures appropriate for each activity being conducted (see Clause **6**). Staff shall be suitably trained and shall be deemed competent to carry out the screening activities. Emergency procedures shall be initiated if at any point during screening an item is considered suspicious. Recommended actions upon discovery of any suspicious delivered item are given in Annex B.
1	• External visual inspection of every item. • X-ray anything of concern, especially larger items (packets, parcels, etc.).	Moderate	Low	
2	• X-ray all items in bulk/large batches initially. • X-ray again individually or in smaller batches if anything anomalous is observed.	Very good to excellent	Low	
3	Level 2 followed by: • External visual inspection of every item. • For each item, tap to encourage any powders or similar materials to move to one edge/corner, and feel for presence of any such anomalies. • For any items identified as anomalous, open side of envelope or packaging by cutting, and without removing, examine contents visually; remove contents.	(Negligible further benefit)	Low to moderate	
4	Level 2 followed by: • External visual inspection of every item. • For each item, remove a corner of the envelope/packaging by cutting; tap gently to encourage any powders or other materials and small items to move to that corner, and inspect visually for presence of any such anomalies. • For any items identified as anomalous, open side of envelope or packaging by cutting, and without removing, examine contents visually; remove contents.	(Negligible further benefit)	Moderate to good	
5	Level 2 followed by: • External visual inspection of every item. • For each item, open side of envelope or packaging by cutting, and without removing, examine contents visually; remove contents if satisfied safe to do so; inspect outer wrapping and contents for any further evidence of powders and other anomalous items or materials.	(Negligible further benefit)	Very good	

***NOTE 4** The larger the volume of mail X-rayed at once, the harder it will be to find smaller threat objects. Mail should therefore be screened in batches, sized so as to provide clear images allowing unambiguous interpretation by the operator.*

***NOTE 5** It is also important to ensure that the volume of material placed in the X-ray machine does not exceed the volume that the system can image; this particularly applies to cabinet X-ray systems.*

6 Physical protective measures

Having identified and assessed all the organization's mail streams and decided appropriate screening levels for them, the organization shall specify and implement the necessary screening and security measures and facilities.

The location of the screening facility (see **8.5**) shall, as far as possible, be chosen with the aim of reducing the likelihood of an incident adversely impacting on the organization's business, or its neighbours.

NOTE 1 A general order of preference for screening locations is therefore:

a) offsite (most preferable);

b) dedicated mail facility at site perimeter;

c) mail room within larger building but with its own external door (through which mail is delivered, and incidents can be resolved whilst limiting the impact on the rest of the building, and minimizing the spread of any contamination);

d) mail room near a minor (e.g. service) entrance to building (through which mail is delivered, and incidents can be resolved; locating the mail room near a main entrance should be avoided);

e) mail room in the heart of a building (not recommended).

NOTE 2 If the location of the screening facility is, for any reason, less than ideal, it is particularly important that the resulting risks are mitigated through careful selection and application of appropriate physical measures.

A series of formal physical protection classes (A to D) is outlined in Table 2. These comprise incremental physical measures intended to protect the organization and its personnel and facilities from increasingly severe postal hazards. These measures predominantly relate to the design, construction (including ventilation) and layout of the mail room, but also include personal protective measures.

The organization shall decide and record which physical protection class from Table 2 is to be applied to each of its various mail streams, and implement the appropriate measures robustly and with regular review. As part of this process, the organization shall also consider potential future requirements both with regard to changes to the threat climate and to changes to mail streams.

Table 2 – Physical protection classes

Physical class	Aim	Minimum physical protective measures for mail room protection
A	To minimize disruption to the organization in the event that a suspected discrete threat object or bulk material is found in mail, or a small explosive device activates (for example within a letter or small packet). It offers negligible protection against "white powder" hazards. It is likely to be most suitable for organizations that are relatively unlikely to be targeted, and handle small to moderate volumes of mail.	Unless mail is screened in a dedicated building remote from other occupied buildings or operational infrastructure, any room in which mail is X-rayed shall be constructed sufficient to withstand, as a minimum, the blast from a typical smaller postal device (e.g. letter or smaller packet). *NOTE 1 Whilst all mail screening could take place in one room, multiple rooms should be considered if high volumes of mail are to be processed, and especially if mail is to be X-rayed.* *NOTE 2 Specialist security engineers should be involved in the design process and oversight of any construction work (See Bibliography for information on the Register of Security Engineers and Specialists).*

Table 2 – Physical protection classes *(continued)*

Physical class	Aim	Minimum physical protective measures for mail room protection
B	To minimize the disruption to the organization in the event that a suspected discrete threat object or bulk material is found in mail, or a larger postal explosive device activates (for example within a larger packet or small parcel). In addition, it offers moderate protection against "white powder" hazards. It is likely to be most suitable for organizations handling moderate to large volumes of mail.	Unless volumes of mail are very low, the facility shall comprise multiple rooms. This will allow different tasks to be carried out in different workspaces, and could offer resilience in the event of a minor incident. Unless mail is screened in a dedicated building remote from other occupied buildings or operational infrastructure, any room in which mail is X-rayed shall be of a hardened and vented construction, designed (see Annex C) to withstand the blast from a typical larger postal device (e.g. larger packet or small parcel). ***NOTE 3*** *Specialist security engineers should be involved in the design process and oversee any construction work.* ***NOTE 4*** *Consideration should be given to locating any X-ray screening machine in a dedicated room, with the facility to operate the X-ray machine remotely thereby protecting the operator and colleagues.* ***NOTE 5*** *All furniture and equipment within the mail room facility (other than any which is specifically designed to be mobile or portable), including tables, other work surfaces, pigeonholes, should be securely fixed to the floor and/or wall to prevent movement. However, nothing should be fixed to the outer faces of the X-ray room walls and any furniture should be at least 300 mm away from them (see Annex C).* The workspace shall be designed and maintained so as to facilitate cleaning. ***NOTE 6*** *The workspace, including floors, walls and work surfaces should be designed and maintained so as to facilitate and withstand thorough cleaning, including decontamination following a release of hazardous material. All corners should be smoothly curved to facilitate cleaning; electrical outlets, switches, controls, light fittings, etc, should be specified as IP64 which affords "dust tight" protection and protection from "water splashes from all directions" in accordance with BS EN 60529:1992.* ***NOTE 7*** *Rooms should be designed with the minimum number of air gaps and apertures; for example: doors should be close-fitting; there should be no significant gaps between wall sections and/or the floor/ceiling; there should be no unsealed cable/service apertures.* Heating, Ventilation and Air Conditioning (HVAC) systems shall be designed so that air flows in and around the mail facility minimize the spread of any contaminant release. If the mail facility is within a larger building it shall have dedicated HVAC circuits and pressure gradients shall be such that air will flow into the facility from the rest of the building. The external air inlets and exhausts from mail room HVAC systems shall be located as far as possible from any other air intakes, windows, etc. The organization shall ensure that emergency procedures for responding to postal incidents include clear and appropriate instructions regarding stopping or sealing off the specific HVAC system employed. ***NOTE 8*** *Specialist HVAC engineers who are members of the Register of Security Engineers and Specialists (RSES) or are able to demonstrate competencies similar to those required for RSES membership should be consulted if system- or location-specific guidance is required.* Facilities for hand-washing shall be available within or nearby the mail room complex.

Table 2 – Physical protection classes *(continued)*

Physical class	Aim	Minimum physical protective measures for mail room protection
C	To minimize the disruption to the organization in the event that a suspected discrete threat object or bulk material is found in mail, or a larger postal explosive device activates (for example within a larger packet or small parcel). In addition, it offers a good level of protection against "white powder" hazards both to the organization's facilities and its staff. It is likely to be most suitable for organizations that are moderately likely to be targeted and handle moderate to large volumes of mail.	Those facilities which operate within physical protection class C shall meet all the requirements in class B, together with the following requirements: *NOTE 9 Specialist security engineers should be involved in the design process and oversee any construction work (see Bibliography for information on the RSES).* Different tasks (e.g. X-ray screening, mail opening) shall be carried out in different rooms, with rooms designed, constructed and finished accordingly. Any X-ray screening machine shall be located in a dedicated room, with the facility to operate the X-ray machine remotely, thereby protecting the operator and colleagues. The minimum number of people necessary to carry out the required work shall be present when mail is cut or opened and subsequently inspected. Rooms shall be designed with the minimum number of air gaps and apertures. Doors shall be close-fitting; there shall be no significant gaps between wall sections and/or the floor/ceiling; there shall be no unsealed cable/service apertures. The workspace, including floors, walls and work surfaces shall be designed and maintained so as to facilitate and withstand thorough cleaning, including decontamination following a release of hazardous material. *NOTE 10 All corners should be smoothly curved to facilitate cleaning; electrical outlets, switches, controls, light fittings, etc, should be specified as IP64 which affords "dust tight" protection and protection from "water splashes from all directions" in accordance with BS EN 60529:1992.* All processes involving cutting or opening of mail shall be carried out in suitable CBR safety flow cabinets with HEPA filtration of their exhaust air flows (most applicable to higher volumes of lower risk mail) or suitable glove boxes (most applicable to smaller volume, higher risk mail streams). All personnel working in rooms where mail is cut or opened shall wear appropriate personal protective equipment (PPE); an assessment shall be conducted to determine what PPE is suitable. *NOTE 11 The Personal Protective Equipment at Work Regulations 1992 require every employer to provide suitable PPE to each employee who might be exposed to any risk whilst at work, except where any such risk has been adequately controlled by other means which are equally or more effective. PPE that could be considered in this context includes: respiratory protection, eye protection, gloves, overalls and footwear. See Bibliography for details of sources of further information.* Rest room facilities shall be available within the mail room complex and shall include a telephone, hand-washing facilities and changing rooms for putting on and removing PPE. *NOTE 12 Restroom facilities should also include toilets and showers.*

Table 2 – Physical protection classes *(continued)*

Physical class	Aim	Minimum physical protective measures for mail room protection
D	To minimize the disruption to the organization in the event that a suspected discrete threat object or bulk material is found in mail, or a larger postal explosive device activates (for example within a larger packet or small parcel). In addition, it offers a very good level of protection against "white powder" hazards both to the organization's facilities and its staff. It is likely to be most suitable for organizations that are likely to be targeted, and handle moderate to large volumes of mail.	Those facilities which operate within physical protection class D shall meet all the requirements in classes B and C, together with the following requirements. ***NOTE 13** Specialist security engineers should be involved in the design process and oversee any construction work (see Bibliography for information on the RSES).* The mail room shall have a specialist HVAC system with HEPA filtration and air flows in workspaces designed to protect personnel as they handle and open mail; the system shall be designed so that pressure gradients between rooms minimize the spread of any contaminants; the system shall incorporate HEPA filtration of the exhaust air flow. ***NOTE 14** This level of HVAC performance should remove the need, required at Class C, to open mail in laminar flow cabinets or glove boxes, except in the case of items of mail that are suspected of containing "white powder" hazards.* ***NOTE 15** Consideration should also be given to including chemical filtration of the HVAC system exhaust air flow.* The workspace (including rooms, floor coverings, fixtures, fittings and furniture) shall be designed to enable deep cleaning or decontamination in the event of a spillage or other release of hazardous material. Full restroom facilities shall be available within the mail room complex; these shall be designed to serve the additional purpose of being a safe refuge for staff whilst they await the emergency response following exposure to suspected contaminants. The restroom area shall include a telephone, hand-washing facilities, changing rooms, toilets and showers.

***NOTE 3** The organization should aim to adopt a physical protection class appropriate for the chosen level of screening. The recommended minimum physical protection classes for each screening level are set out in Table 3. These are given as recommendations because constraints, such as the location and construction of existing mail room facilities, could prevent adoption of some aspects, at least in the short- to medium term. Where such constraints are encountered, specialist security engineers should be consulted as they might be able to propose alternative protective measures suited to the specific situation.*

Table 3 – Recommended minimum physical protection classes for each screening level

Screening level	Recommended minimum physical protection class
1	A
2	A to B
3	C
4	C to D
5	D

NOTE 4 It will generally be substantially easier to change screening levels than to change the physical protection class of a particular facility. A mail room should therefore be designed and constructed to a class appropriate for the highest anticipated screening level that may be required.

NOTE 5 In addition to the protection afforded by implementing the measures associated with a particular physical protection class, the choice of location of the mail facility also contributes to the overall level of protection. Protection can usually be improved by moving mail handling and screening activity away from significant operational or otherwise critical areas. Options include using a dedicated facility near the site perimeter, or an offsite location.

The organization shall therefore consider, informed by its analysis of postal threats and their potential impact, where mail screening and handling activity is best located.

NOTE 6 If the organization screens mail at level 5, with facilities meeting physical protection class D and located offsite, it could derive still further protection by scanning all suitable written contents into a digital format and forwarding this electronically to the recipient; this will significantly reduce the risk of trace "white powder" contamination reaching operational buildings. If this process is adopted, original documents should be retained for a specified period before secure destruction and disposal; all other items should be thoroughly inspected manually before being forwarded to the recipient.

In addition to the screening measures, the organization shall also specify and implement appropriate general postal security measures. These can safeguard mail containing valuable items and sensitive information, and can also contribute to the integrity of the screening capability.

7 Summarizing the organization's requirements

The organization shall formally record its requirements for mail screening and security in sufficient detail to enable unambiguous implementation either by its own staff, or by a contractor. This record shall include:

- a summary of the organization's understanding of its mail streams, including likely volumes and timing constraints;
- a summary of the threats the organization faces, and the potential of these to change the required screening level for each mail stream;
- the required level of screening for each mail stream;
- the physical protective measures associated with the mail handling and screening processes;
- the location of the mail screening activity;
- other general postal security measures.

***NOTE 1** Taking a more holistic approach and capturing wider aspects of mail handling and security, such as sorting, and delivery of items to recipients, can help ensure the required screening approach is practical.*

Any mail stream that is identified as warranting screening shall be screened in its entirety.

***NOTE 2** As screening is intended to give confidence that a mail stream does not contain hazardous items or materials, there is little rationale for screening only a proportion of a particular stream. Also it is important to note that as mail screening is typically a low profile security measure it might not offer the deterrent effect that other more visible security measures (such as visitor screening regimes) may provide.*

Screening and security measures shall be appropriate for the likelihood and type of postal attack threats to the organization and their potential impact. The organization's screening capability shall be flexible: it shall be able to cope with the need to increase the level of screening at times of heightened threat.

Screening capacity shall be sufficient to cover anticipated maximum throughputs.

***NOTE 3** For each mail stream, it is important to know the volume of mail received and understand how this may vary; for example, streams may vary weekly, seasonally or otherwise according to the nature of the organization's business.*

The organization shall understand the relative priorities of, and timings associated with, its mail streams, and in particular what the maximum time available for screening is for each particular stream.

***NOTE 4** It may be acceptable, for example, that at times of heightened threat, and hence higher required screening level, lower priority streams can be screened later in the day than would normally be the case.*

There is an increased risk associated with imposing a significant delay between receipt and screening; consideration shall therefore be given to conducting an initial, more basic bulk screening step as soon as possible following receipt.

The organization shall encourage a good level of awareness and vigilance of all staff regarding mail they receive at their workstations; this can provide a rudimentary level of screening that will benefit all organizations and may in some cases even be sufficient screening. The effectiveness of such an approach depends heavily on awareness of the threat and how to respond in the event that an item of mail causes concern; staff shall receive regular reminders.

8 Implementation

8.1 General

Once the organization's requirements for mail security and screening capability have been formally stated, the following aspects of implementation shall be addressed:

- general postal security measures (see **8.2**);
- management and responsibility, including any decision regarding internal versus outsourced operation (see **8.3**);
- operating procedures (including emergency procedures) (see **8.4**);
- mail room/screening facility – location and design, layout and construction (see **8.5** and Annex C);
- screening methods and equipment (see **8.6**);
- human factors (see **8.7**);
- health and safety considerations (see **8.8**).

***NOTE** Many elements of these strands are inter-related, hence they should not be addressed in isolation; this is particularly relevant to the consideration of health and safety which should be an integral part of the entire implementation process.*

8.2 General postal security measures

Based on its understanding of its mail streams (see **4.3**), the organization shall identify and implement appropriate measures to ensure the general security of all items of mail, together with any additional measures deemed necessary to protect valuable items and sensitive information.

***NOTE 1** Sensitive information on electronic media should be sent in an appropriate encrypted format.*

The organization shall ensure appropriate general physical security measures (including, for example, access control and CCTV) for areas where mail is handled and stored, combined with good practice personnel security measures for those involved in mail handling.

***NOTE 2** Good practice guidance on physical, cyber and personnel security measures can be found at www.cpni.gov.uk.*

The organization shall review the extent to which it needs to send and receive valuable items and sensitive information by mail.

Valuable, sensitive and otherwise important items in the organization's mail streams shall be safeguarded to an appropriate extent.

***NOTE 3** Measures may include creation of dedicated, low volume mail streams for such items, and tracking (and formally recording) the progress of items at all stages between sender and recipient. For example, all items entering the organization from external tracked services should be logged on entry, tracked through the screening process, and delivered directly to the recipient who should sign to acknowledge receipt.*

***NOTE 4** Whilst the organization only has direct control over mail actually in its care, it could be able to extend this control through formal arrangements with trusted contractors, for example using tracked services for outgoing items, or even dedicated deliveries or collections for particularly important items.*

8.3 Management and responsibility

As with all other aspects of security, there shall be clear and appropriate management responsibility for postal security and screening requirements and implementation, even where this activity is contracted out. Management responsibility shall include regular review, evidence of which shall be formally recorded. Management responsibility shall be formally detailed in the operating procedures for mail screening, handling and associated security measures (see **8.4**).

There shall be high level management commitment to postal security and screening within the organization; this shall be clearly communicated to staff at all levels.

Postal security shall not conflict significantly with other organizational targets.

***NOTE 1** For example, if a member of staff reasonably identifies an item as causing concern, he/she should not then be penalized for any lack of productivity associated with the time taken to resolve the incident.*

An important management issue is the decision whether to operate any postal screening capability within the organization or contract it out. As there are significant points both in favour of and against each option, the organization shall consider the implications of each thoroughly before making a final decision.

NOTE 2 Operating the capability within the organization maximizes visibility and control over it, and ensures it is an integrated part of the organization's overall security measures that can be adjusted as appropriate in response to any relevant changes.

NOTE 3 Mail screening and security is viewed by many organizations as a non-core activity. Contracting it out to a facilities management provider or a specialist postal services provider, can therefore be attractive from a management perspective.

If considering outsourcing, the organization shall state its requirements in sufficient detail to enable unambiguous implementation by a suitable contractor.

When assessing bids, particular attention shall be paid to elements such as emergency procedures, contingency plans and human factors issues.

NOTE 4 Assessing the relative merits of different commercial offerings at the bid stage should be challenging, though clearly stated requirements will help significantly.

Outsourcing might remove mail screening to an offsite location, which reduces the likelihood of a mail-related incident affecting core business; in such instances, the security of the mail after it is screened shall warrant particular attention.

NOTE 5 Outsourcing might, depending on the provider, offer greater or lesser flexibility to change throughputs or levels of screening as events dictate. Monitoring ongoing performance of the outsourced service could also be difficult. These and other issues might usefully be addressed through a service level agreement between the organization and its contractor, with relevant metrics formalized as key performance indicators.

NOTE 6 This PAS does not address the requirements for establishing liability should the screening process fail, but it is considered advisable that any legal agreement between two parties recognizes the possibility of service failures.

Where the organization occupies shared premises, its management shall conduct an assessment of the wider postal security risks arising from this arrangement, and shall implement postal security and screening measures accordingly.

The organization's management shall regularly review mail screening capability and security measures, as well as the context in which the organization operates; such reviews shall include checks that actual screening processes are in accord with documented measures.

In addition, whenever there is a material change to the organization or the threat, the organization shall review the risks associated with its mail security, and where required go on to review its mail screening capability and security measures.

8.4 Operating procedures (including emergency procedures)

The organization shall have clear, formally recorded, operating procedures for mail screening, handling and associated security measures; these shall describe the screening and handling processes, how they are managed, and the locations in which they take place. The procedures shall address all mail streams and describe in detail how each stream is to be screened at the required level (see Clause **5**) and with the required class of physical protection (see Clause **6**). When drawing up these procedures, consideration shall be given as to whether detailed provision is made for enhanced levels of screening to be implemented at times of heightened threat.

The operating procedures shall include emergency procedures for managing any incidents.

NOTE 1 Sources of advice and information on security planning are included in the Bibliography.

NOTE 2 General guidance on how to respond to the identification of a suspicious postal item is provided in Annex B.

In the event that a suspicious postal item is found, it shall not be moved from the location where it is found. The suspicious postal item shall be isolated, and individuals in the same room shall be requested to leave the room and proceed to a segregated area away from other individuals.

The organization shall consider implementing a process for recording all incidents involving mail being identified that causes (or has the potential to cause) concern, disruption or harm, either during screening or elsewhere. Such a process shall involve sufficient detail being collated in a timely manner about the nature of each incident and the associated response that it can contribute both to the organization's current understanding of the threat it faces, and to periodic review of screening requirements and capability.

NOTE 3 *The organization might wish to consider making incident details available to all elements of the organization which would receive learning or awareness benefit.*

The operating procedures shall be consistent with wider security measures employed in the organization. In particular, the emergency procedures for managing postal incidents shall form part of, and be consistent with, the organization's wider emergency procedures.

The organization shall ensure that its emergency procedures clearly describe management responsibility in the event of an incident, as well as detailing how decision making is to be escalated.

NOTE 4 *The organization might wish to consider marking items of mail that have been screened, for example, with a date stamp of a specific design. This could contribute towards the general security of mail and quality assurance of the screening process.*

The organization shall ensure that the operating procedures (including the emergency procedures) are accessible to and understood by all relevant staff. The organization shall determine the appropriate level and frequency of training and rehearsing of emergency procedures (noting that requirements might vary with role, location, etc.) and shall adhere to this. Training and rehearsing of emergency procedures shall achieve an appropriate balance of addressing the principal issues and the more minor details. An auditable record shall be kept of training and exercising activity.

The organization shall ensure that emergency procedures address both incidents arising during formal screening and mail handling (i.e. by specialist staff and probably in dedicated mail room facilities) and incidents that might occur elsewhere (in particular where mail is opened by general staff at their workstations). For the latter case, the organization shall have simple clear procedures that all staff within the organization are aware of (and regularly reminded of), on how to respond to a suspicious postal item.

The emergency procedures shall take account of factors such as the location and physical construction of the mail room. Particularly detailed consideration shall be given to evacuation requirements if the mail room is located within a major operational building.

If mail handling and screening is outsourced, the organization and its contractor shall each have appropriate and adequate operating and emergency procedures covering their respective activities.

The organization shall have overall responsibility for ensuring that these are, and continue to be, complementary and collectively address all relevant issues. The same points shall apply where the organization occupies shared premises.

The organization shall ensure that the operating procedures adequately address the general security of mail while it is transported, stored and otherwise handled within its boundaries, so as to minimize the likelihood of loss, theft, damage or tampering.

All procedures shall be reviewed regularly and updated as required; the organization shall set a defined frequency for such reviews, dependent upon the needs of the business, and this shall be adhered to. In addition, all procedures shall be reviewed following any material change to the organization, its mail streams, or the wider threat context. The effectiveness of the emergency procedures and their implementation shall be reviewed following any incident.

The organization shall have contingency plans in case a postal security incident affects operation of the mail room or other parts of the organization; these need not be stand-alone and could form part of the organization's wider contingency plans or business continuity plans.

NOTE 5 *The organization's contingency planning should also take account of how other incidents might impact on mail screening and handling requirements and capability.*

8.5 Mail room/screening facility

8.5.1 Location

Mail shall be screened as soon as reasonably possible after it is delivered.

The location of the screening facility shall, as far as possible, be chosen with the aim of reducing the likelihood of an incident adversely impacting on the organization's business, as well as without adversely affecting its neighbours.

NOTE 1 *This should be achieved through a combination of screening mail as early as possible following receipt,* *and as far away as possible from locations that might be adversely affected by an incident involving a suspect item.*

***NOTE 2** A general order of preference for screening locations is therefore:*

a) offsite (most preferable);

b) dedicated mail facility at site perimeter;

c) mail room within larger building but with its own external door (through which mail is delivered, and incidents can be resolved whilst limiting the impact on the rest of the building, and minimizing the spread of any contamination);

d) mail room near a minor (e.g. service) entrance to building (through which mail is delivered, and incidents can be resolved; in accord with Note 1, locating the mail room near a main entrance should be avoided);

e) mail room in the heart of a building (not recommended).

***NOTE 3** For multi-occupancy buildings consideration should be given to coordinating mail screening arrangements to ensure risks are appropriately and consistently addressed. This might be most effectively addressed by one mail room screening the mail for all occupants.*

Different hazards have different potential implications that shall be considered when planning the location and construction of a mail room.

***NOTE 4** For example, explosives hazards could impact on critical fragile elements of a building or its contents (e.g. structural components or IT infrastructure), whilst certain chemical, biological and radiological materials could cause widespread contamination.*

***NOTE 5** Identifying and implementing the appropriate screening levels and physical protection classes should help ensure that the screening process and associated protective measures are commensurate with the risks the organization faces.*

***NOTE 6** The cost of moving or changing existing facilities may be prohibitive and/or excessive when compared with the risk a particular organization faces. However, refurbishment or new-build projects can offer good opportunities to make radical changes to existing security measures, and these should not be overlooked. It may also be possible to offset costs with other operational benefits. For example, moving a mail room offsite may be costly, but may free up much needed space in a headquarters building that can instead be used for core business activity.*

8.5.2 Design, layout and construction

The mail room shall have adequate space for current and anticipated screening, sorting and related mail handling activities. The layout shall, as far as possible, be configured in a way that logically reflects the required screening and handling activities. As much of the work is likely to be repetitive and potentially tedious, the layout and work processes shall also be reviewed from an ergonomic perspective.

The mail facility shall be designed and constructed with appropriate physical protection measures. Table 2 outlines the measures that shall be adopted commensurate to the required physical protection class for the facility.

***NOTE 1** Specialist security engineers should be consulted where the organization requires more detailed advice on these matters.*

Whilst new facilities shall as far as possible be designed around the mail screening and handling processes they are to accommodate, and so have an appropriate physical protection class, this might not always be achievable where pre-existing facilities are to be used.

The design, layout and construction of the mail room shall be such that it is easy to keep tidy. Maintenance of the mail room in a clean and tidy state shall be addressed through operating procedures, supported by regular management review and inspection.

Access to the mail room shall be controlled, limiting entry to authorized individuals directly involved in mail screening and handling, and maintenance of the facility.

The organization shall consider whether there is a requirement for redundancy of capacity for mail screening and handling, for example, for business continuity purposes.

NOTE 2 *This could be achieved in a number of ways, including use of multiple facilities in separate locations that could be used interchangeably, or designing the mail room such that a minor incident that suspends activity in one area does not necessarily prevent continued operation of other areas.*

Effective communication is an important element of managing emergencies and incidents. A mail room facility shall have at least one telephone for use in emergencies.

NOTE 3 *It is recommended that there should be one telephone in each significant room in the facility, including any restroom.*

NOTE 4 *CCTV should be installed that provides high quality images of all working areas within the mail room. In addition to being a basic security measure, it can be a valuable tool during the management of any incident within the mail facility and for post-incident investigation.*

8.6 Screening methods and equipment

Those responsible for the management of mail screening within an organization shall develop and implement a written procedure for how mail is to be screened for each of the levels assessed as relevant or potentially relevant to the organization (see Table 1). The emphasis shall be on the overall screening process; whilst technology could contribute significantly to the process, it shall not be considered in isolation. This written procedure (or procedures) shall form part of the overall operating procedure for mail screening and handling within the organization.

Protective equipment, as outlined in Table 2, shall be identified and used as appropriate for the chosen physical protection class. This shall be documented in the procedure.

NOTE 1 *Depending on the nature of the organization's business, it may receive greater or lesser quantities of more complex items of mail that are difficult to screen, for example, because they provide cluttered images when X-rayed. In addition to the use of further screening measures, other checks might be used to inform the screening decision for each item.*

Any checks or measures used to inform screening decisions (e.g. checks that an item matches an order on the organization's procurement database, or the addressee confirms that it is expected) shall, where appropriate, be included in the organization's operating procedure for mail screening. Screening methods shall be designed to ensure that mail streams do not become mixed where it would be detrimental to do so, and that the scope for any contamination to be spread is otherwise minimized. For example, screened mail shall be clearly separated from unscreened mail; mail streams requiring a high level of screening shall not be mixed with streams requiring lower level screening.

NOTE 2 *The only screening technology specifically included in this PAS is mail X-ray screening; a wide range of such systems are commercially available that, if used according to manufacturers' instructions and by trained and experienced operators, can provide a good level of screening capability. There are two relevant forms of X-ray machine marketed for postal screening:*

- *cabinet X-ray machines (also known as fluoroscopes), in which mail is placed manually in a compartment within the machine; these tend to be suitable for moderate throughputs of mail;*

- *conveyorized X-ray machines (also known as linescan systems), similar to those used in aviation security; these could be used to screen high throughputs of mail.*

NOTE 3 *Additional information on X-ray machines for mail screening, including minimum recommended performance standards, are provided in Annex D; information on the design, layout and construction of rooms in which X-ray screening is to be conducted is provided in Annex C.*

NOTE 4 *Having the capability to view X-ray images remotely can assist with the management and resolution of incidents.*

Staff shall understand and gain experience both of how to operate the equipment and of how to use it to identify and/or discount threats.

NOTE 5 *Whilst various other detection technologies are available, individually they tend only to offer capability against a very small proportion of the overall spectrum of potential threat materials and items. Decisions surrounding the selection and implementation of such technologies are therefore particularly complex, and fall outside the scope of this PAS.*

8.7 Human factors

8.7.1 General

As with other aspects of security, the vigilance and awareness of staff is key to the success of postal screening and security measures. Whilst this is particularly applicable to staff involved in mail handling and screening, it also has much wider relevance, which should not be overlooked.

The organization shall ensure that all staff who might receive mail at their workstations are aware of how to identify and respond to suspicious postal items. This shall be achieved through clear, straightforward and well communicated procedures, supported by awareness raising at appropriate intervals.

NOTE *A list of possible indicators that a delivered item may be of concern is presented in Annex A. General guidance on how to respond to the identification of a suspicious postal item is provided in Annex B.*

As the screening process relies upon the vigilance and awareness of human operators, the organization shall do everything possible to encourage their optimum performance.

8.7.2 Personnel security

The organization shall implement good personnel security practice for staff involved in the handling and screening of mail.

NOTE *Good practice guidance on personnel security can be found at www.cpni.gov.uk.*

8.7.3 Ergonomic considerations

The workspace and mail handling and screening processes shall be designed as far as possible to take account of ergonomic considerations relevant to maximizing the effectiveness of the screening process.

NOTE *Ergonomics experts with relevant experience should be consulted where the organization requires advice on such matters.*

8.7.4 Training

Staff shall be trained in the screening methods they are implementing (including use of any equipment), awareness of the broad range of threats they might encounter, and in the emergency procedures. They shall receive refresher training at appropriate intervals, and as required in light of any changes, for example, to the threat or to the screening procedures or equipment.

NOTE *In addition to refresher training, supplementary training might also be required following any incidents.*

8.7.5 Staff motivation

Disaffected staff might cut corners, potentially reducing the effectiveness of the screening processes. The organization shall endeavour to ensure that staff remain well motivated, and encourage line managers to avoid conflicting demands, confusing messages, and look out for signs of reduced motivation in staff.

NOTE *For example, unreasonable throughput targets with actual or implied penalties might encourage screeners to cut corners.*

8.7.6 Effectiveness

It is recognized that many security tasks are repetitive and tedious; screening effectiveness can be assumed to be reduced if staff focus on particular tasks for too long. Screening procedures shall address this through ensuring staff rotate between tasks regularly and take appropriate breaks.

NOTE 1 *Task rotation should also offer the additional benefit of redundancy of capability.*

Screening procedures shall include provision for assessing and monitoring the performance of the process.

NOTE 2 *Testing the mail screening process, for example using dummy threats, should be considered, though care should be taken to ensure this is managed properly.*

8.8 Health and safety considerations

A comprehensive health and safety risk assessment shall be conducted for the mail handling, screening and security process. The implications of the organization and its staff receiving and handling mail that might be hazardous shall be considered as part of this. Particular attention shall be paid to hazards arising directly from the screening process.

NOTE *Particular care should be taken when mail handling and screening activity is outsourced to ensure that health and safety considerations (including risk assessments and safe systems of work) are adequately addressed by both the organization and its contractor (see* ***8.3****).*

Annex A (informative)
Possible indicators that a delivered item may be of concern (from www.cpni.gov.uk)

Many of the listed indicators are quite general. One alone will not necessarily constitute a cause for concern. Their individual relevance will vary with context, e.g. depending on the nature of the organization's business, and in light of the current threat and Response Level. Any suspicions should be considered in combination with a thorough risk assessment.

General indicators

General indicators that a delivered item may be of concern include:

- unexpected item, especially if hand delivered;
- a padded envelope ("Jiffy Bag") or other bulky package;
- additional inner envelope or other contents that may be difficult to remove;
- labelling or excessive sealing that encourages opening at a particular end or in a particular way;
- oddly shaped or lopsided;
- envelope flap stuck down completely (normally gummed envelope flaps leave slight gaps at edges);
- marked "to be opened only by...", "personal" or "confidential";
- item addressed to the organization or a title (rather than a specific individual);
- unexpected or unusual origin (postmark and/or return address);
- no return address or a return address that cannot be verified;
- poorly or inaccurately addressed;
- address printed unevenly or unusually;
- unfamiliar writing or unusual style;
- unusual postmark or no postmark;
- more stamps than needed for size or weight of package;
- greasy or oily stains emanating from package;
- odours emanating from package.

Explosive or incendiary indicators

Additional explosive or incendiary indicators include:

- unusually heavy or uneven weight distribution;
- small hole(s) in envelope or wrapping;
- presence of wiring.

"White powder" indicators

Additional chemical, biological or radiological (CBR) indicators include:

- powders or liquids emanating from package;
- wrapping stained by liquid leakage;
- marked with written warning(s);
- unexpected items or materials found in package on opening or X-raying (loose or in a container) such as powdered, crystalline or granular solids; liquids; sticky substances or residues;
- unexpected odours observed on opening;
- sudden onset of illness or irritation of skin, eyes or nose.

Annex B (informative) Action upon discovery of any suspicious delivered item (from www.cpni.gov.uk)

You could discover a suspicious item in a mail room, or anywhere else in the building – ensure you have appropriate emergency response plans in place.

Avoid unnecessary handling and X-raying

- If you are holding the item, put it down on a cleared flat surface.
- Keep it separate so it is easily identifiable.
- Do not move it, even to X-ray it.
- If it is in an X-ray facility, leave it there.

Move away immediately

- Clear immediate area and each adjacent room, including rooms above and below.
- If there is any suggestion of CBR materials, move those directly affected to a safe location close to the incident – keep these individuals separate from those not involved.
- Prevent others approaching or accessing the cleared areas.

Do not use mobile phones or two-way radios in the cleared area or within 15 metres of the suspect package.

Communicate regularly with staff, visitors and the public.

Notify police

- If the item has been opened, or partially opened prior to being deemed suspicious, it is vital that this is communicated to the police.
- Ensure informants and witnesses remain available to brief the police, and that the accuracy of their observations is preserved: encourage witnesses immediately to record their observations in writing, and discourage them from discussing the incident or their observations with others prior to the arrival of the police.

***NOTE** The nature, purpose and complexity of heating, ventilation and air conditioning (HVAC) systems varies significantly from building to building, so it is not possible to provide generic advice on whether or not it is best to switch off or isolate systems in the event of a suspected chemical, biological or radiological (CBR) release. Rather, procedures should be formulated on a building-specific basis, with input from specialist HVAC engineers (see Bibliography for information on the RSES).*

Annex C (normative) Mail facility layout and construction to minimize the effects of an explosive device or "white powder"

C.1 Introduction

This Annex is intended to assist those who are required to design and/or provide mail facilities (including rooms for screening, handling, and sorting mail). It details construction requirements necessary to minimize the effects of the blast caused by an explosive device functioning during the X-ray screening process and the consequences arising from finding a "white powder" during the screening process. It aims to address the following requirements:

- to protect the mail room staff from the effects of direct blast and fragments created by an explosive device detonating;
- to protect staff in adjacent corridors and offices (above, below and to the side) from these explosive effects;
- to minimize the impact of a "white powder" incident;
- to prevent significant physical damage to the building and critical systems (a degree of local damage is to be expected).

In designing a mail facility, consideration shall also be given to matters such as ventilation, heating, lighting, power, security systems and fire alarms.

__NOTE 1__ Organizations that receive small volumes of mail and/or are relatively unlikely to be targeted might decide that only basic screening measures, and hence facilities, are sufficient. For example, at Screening Level 1 (see Table 1) all items are subjected to an external visual examination, and any that are deemed of concern are then X-rayed, quite possibly using a smaller, cabinet X-ray system (see Annex D). In such circumstances conducting all mail handling and screening activities in a single room might be proportionate with the risk.

__NOTE 2__ The design of physical protective measures should be informed by an assessment of the threats and the screening methods to be carried out, as defined by the organization. It is recommended that this should be discussed with a specialist security engineer.

__NOTE 3__ The extent of damage and therefore potential injury is dependent on the size of device. This Annex provides general design guidelines which should be adapted to meet the organization's design threat.

For organizations handling larger volumes of mail and/or facing significant threats, the mail facility shall comprise multiple rooms, each housing a separate activity. X-ray screening is likely to involve a conveyorized (linescan) system. The X-ray system shall be located in a separate room to the X-ray operator. Opening mail to screen for "white powders" shall be conducted in a separate room to the X-ray system and X-ray operator.

Ideally mail shall be screened in a dedicated building remote from other occupied buildings or operational infrastructure; however, this is not always practical.

If mail is instead to be screened in part of a larger building, the mail facility shall be located in an area with robust structural framing. X-ray screening shall take place adjacent to an external wall or beneath a frangible roof so that a vent can be provided to release blast pressures in the event that an explosive device functions. Opening mail to screen for "white powders" shall be carried out in suitable CBR safety flow cabinets with HEPA filtration of their exhaust flows (most applicable to higher volumes of lower risk mail) or suitable glove boxes (most applicable to smaller volume, higher risk mail streams), or a room with a HVAC system operating under negative pressure with HEPA filtration of the exhaust air flow.

__NOTE 4__ Alternative locations and designs could be possible but advice should be sought from a specialist security engineer.

C.2 Layout plans

The design for an X-ray screening room depends on the X-ray system chosen (which in turn depends on factors such as the volume of mail to be screened and the size of the largest items to be screened) and the constraints of the building. Figure C.1 shows an example schematic layout for a room housing a conveyorized system; Figure C.2 shows an example layout for a cabinet X-ray facility.

__NOTE 1__ As depicted in Figure C.2, any cabinet X-ray installation should be configured so that the instrument can be controlled remotely. The installation should incorporate a vestibule arrangement to enhance protection against blast effects; doors should be at 90 ° to each other and open in towards the X-ray system.

__NOTE 2__ Where X-ray equipment is in a separate room from the operator, the equipment should be capable *of being operated remotely and an electrical interlock should be provided so that it cannot be operated without the doors being closed.*

Figure C.3 shows an example schematic for a facility housing a "white powder" mail screening room. It corresponds to physical protection Class C (described in Table 2), and is most applicable to higher volumes of lower risk mail. Small volume, higher risk mail streams require substitution of the flow cabinet for a suitable self-contained glove box. Compliance with physical protection Class D (described in Table 2) would require the mail room to have a specialist HVAC system with HEPA filtration and air flows in workspaces designed to protect personnel as they handle and open mail.

C.3 Structural requirements

A postal device detonating inside the postal room will typically result in a confined blast effect. If the device detonates inside the X-ray system, the blast will vent out of each end detaching the lead curtains and projecting them away from the X-ray system. The walls surrounding the X-ray system shall be designed to withstand the confined blast effects and the walls facing the X-ray system openings shall be designed to withstand the additional blast loads focused by the X-ray system and the impact of the lead curtains.

***NOTE 1** Concrete, masonry and lightweight blast resistant wall or partition systems may be used if satisfactory evidence of their performance can be verified. Advice should be sought from a specialist security engineer.*

The floor and ceiling (unless it is a frangible roof) shall be assessed against the design blast loads.

***NOTE 2** Coffered or voided slabs should be avoided.*

C.4 Openings in the X-ray room

A vent aperture (or apertures) permits the blast pressure to dissipate reducing the loads on the walls. Where possible the aperture should be provided through an external wall or the roof. The aperture shall be able to vent into an area 10 m x 10 m which is clear of any major obstructions (e.g. the face of another building). The vent shall be covered by a light frangible sheet with a maximum weight of 20 kg/m^2 and a maximum ultimate failure resistance of 2.0 kN/m^2.

***NOTE 1** Glazing could be used in a vent aperture but it is not recommended.*

***NOTE 2** The vent should not be positioned in line with the end of the X-ray system.*

If personnel can gain access to the area outside the vent aperture appropriate physical security measures shall be implemented to prevent unauthorised entry.

If under a blast load the vent material is likely to become detached and projected, a catcher mesh shall be positioned at least 300 mm from the vent and shall consist of 2 mm diameter wires at 100 mm centres vertically and horizontally and securely tied back to the structure.

If an external access door is present it shall be capable of resisting the design loads. The door shall be locked and alarmed to prevent unauthorized entry.

***NOTE 3** Any such external access door should open inwards towards the X-ray system.*

***NOTE 4** The door should not be positioned in line with the end of the X-ray system.*

The internal access door from the operator's room shall be capable of resisting the design loads. Any such door shall open inwards towards the X-ray system.

***NOTE 5** An electrical interlock should be fitted to the door to prevent operation of the X-ray system unless the door is closed.*

The size of any conveyor hatches between rooms shall be minimized but be of a size compatible with the aperture size of the X-ray system with space for the conveyor system at the bottom. Each hatch shall have a vertical hanging rubber flap curtain to limit the escape of blast pressures.

***NOTE 6** Sealable hatch covers should be provided for use in the event of a release of CBR contaminants.*

***NOTE 7** There should be no HVAC or other services serving or passing through the X-ray room with the exception of any directly required to service the X-ray facility.*

C.5 Openings in other rooms in the mail facility

The doors and windows from the general area of the mail facility into the X-ray operator's room shall be capable of resisting the design loads.

***NOTE** Advice should be sought from a specialist security engineer.*

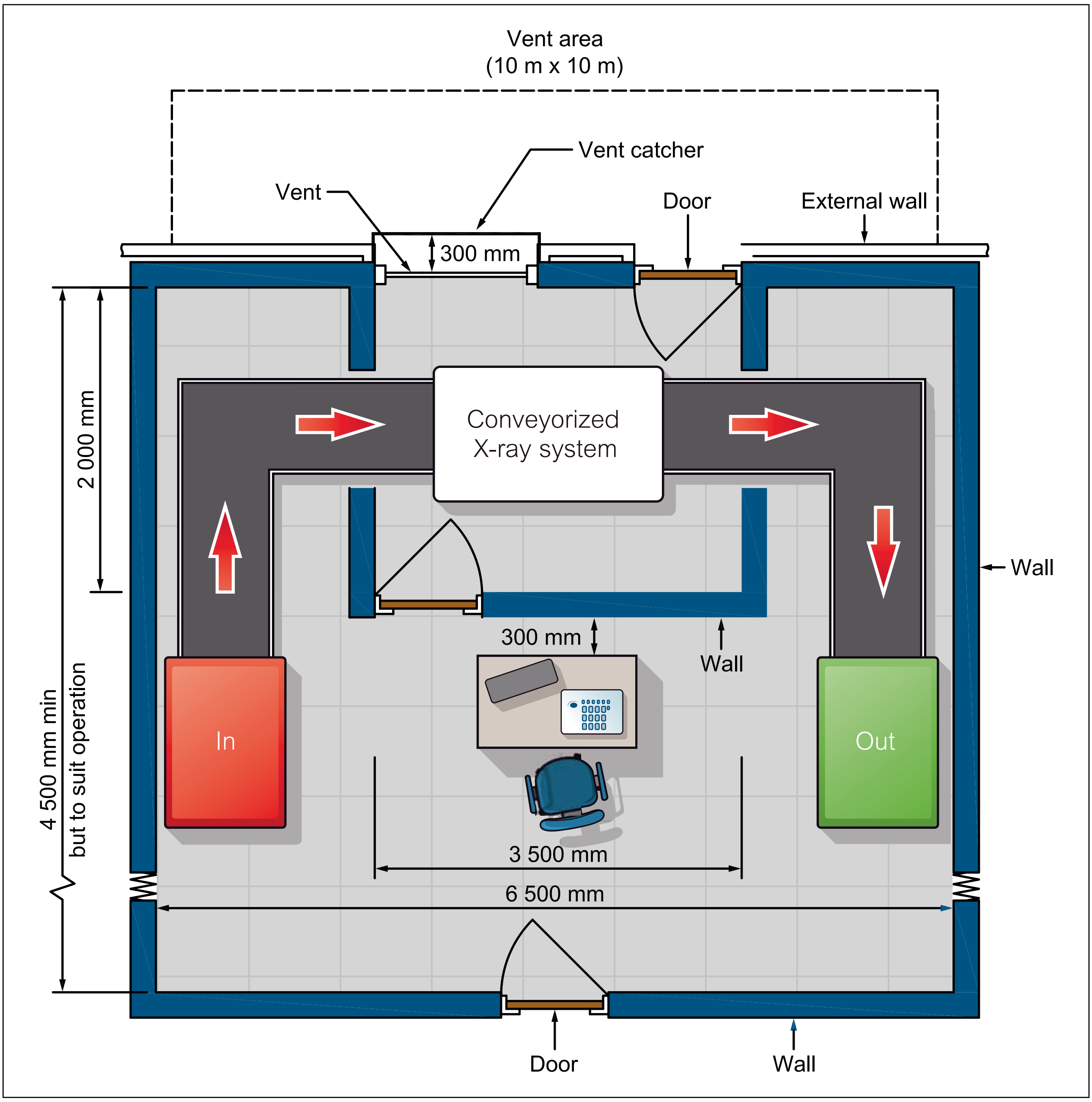
C.6 Other precautions

All windows in direct line of sight and within 30 m of a vent shall be assessed for the effects of a blast within the scanning room. In addition for any elevation with a vent, all windows within a 7 m radius of the vent shall be assessed.

***NOTE** A 300 mm gap should be maintained between the X-ray room wall and any fixtures and fittings in adjacent rooms. This will prevent any objects from being hit by a wall as it deflects, which could cause such items to be dislodged and projected, potentially causing injury.*

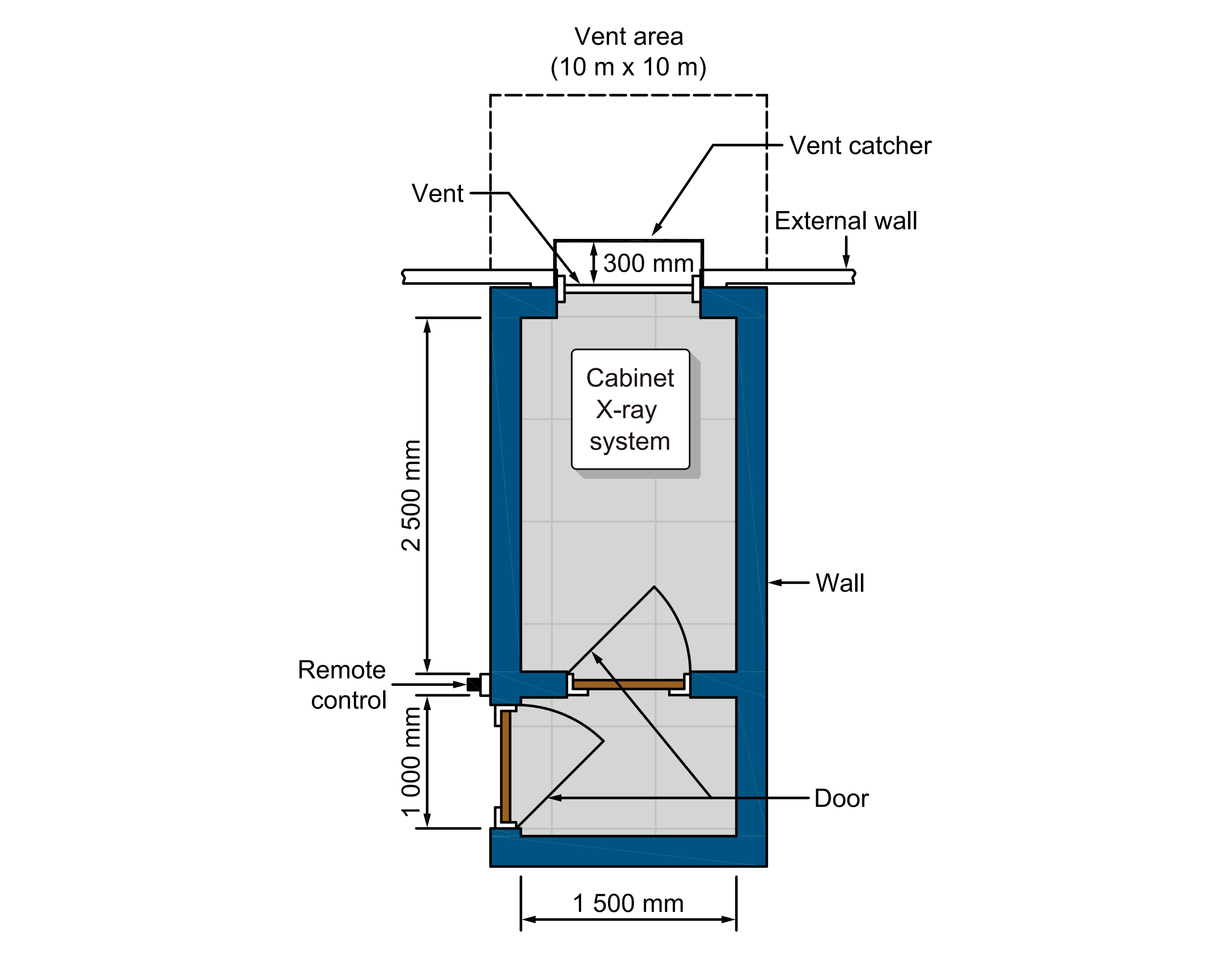
False ceilings shall not be installed in the X-ray or X-ray operator's rooms. Any essential fixtures and fittings (e.g. light fittings) shall be securely fixed and suitably restrained.

Figure C.1 – Conveyorized X-ray screening



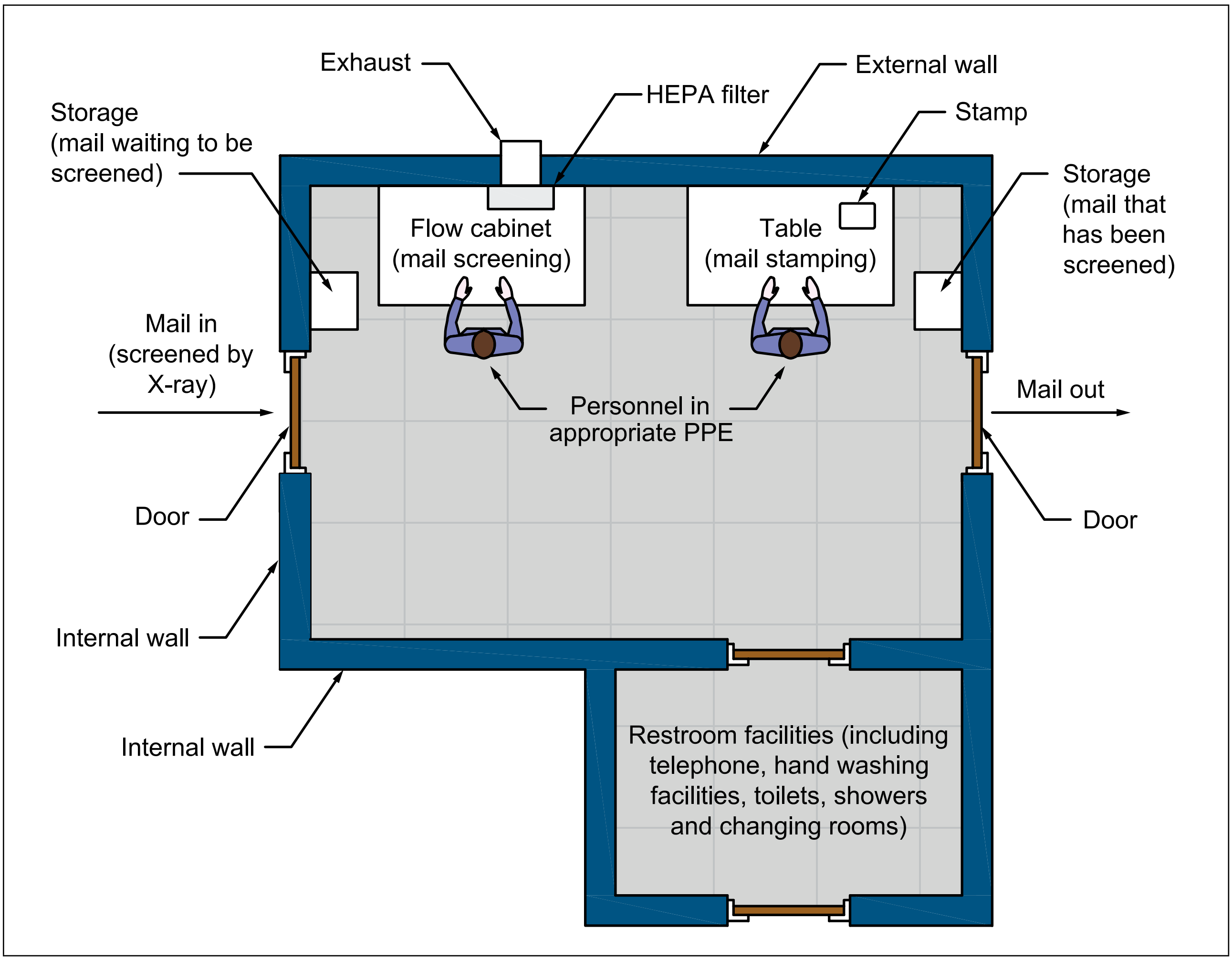
__NOTE__ Dimensions are for guidance only. Diagram is not drawn to scale.

Figure C.2 – Cabinet X-ray screening



***NOTE** Dimensions are for guidance only. Diagram is not to scale.*

Figure C.3 – "White powder" screening


Exhaust
HEPA filter
External wall
Stamp
Storage (mail waiting to be screened)
Flow cabinet (mail screening)
Table (mail stamping)
Storage (mail that has been screened)
Mail in (screened by X-ray)
Personnel in appropriate PPE
Mail out
Door
Door
Internal wall
Internal wall
Restroom facilities (including telephone, hand washing facilities, toilets, showers and changing rooms)

***NOTE** Diagram is not to scale.*

Annex D (informative) Additional information on X-ray machines for mail screening

D.1 Introduction

A wide range of X-ray systems are commercially available that, if used according to manufacturers' instructions and by trained and experienced operators, can provide a good level of mail screening capability. There are two relevant forms of X-ray machine marketed for postal screening:

- cabinet X-ray machines (also known as fluoroscopes), in which mail is placed manually in a compartment within the machine; these tend to be suitable for moderate throughputs of mail;
- conveyorized X-ray machines (also known as linescan systems), similar to those used in aviation security; these could be used to screen high throughputs of mail.

D.2 Mail screening test piece

A standard test piece (STP) is used routinely in the UK aviation industry to monitor X-ray system image quality standards. It is acknowledged that the STP yields useful information about conveyorized X-ray machines for aviation security but this has limitations when applied to mail screening applications. Therefore, a UK mail screening test piece (MSTP) was developed by the Home Office Centre for Applied Science and Technology (CAST), in association with CPNI, for such applications. The UK MSTP is available commercially and is recommended for checking regularly that the system is performing to the expected standard; it does so in terms of:

- single wire resolution;
- ability to resolve a single wire behind varying thicknesses of aluminium;
- spatial resolution in the vertical and horizontal directions;
- imaging metal sheets of varying thickness;
- materials discrimination;
- imaging powders of varying thickness;
- imaging and penetration of paper and paper substitutes of varying thickness.

The tests on the mail screening test piece are designed specifically to cover the full range in capability of both cabinet and conveyorized X-ray machines used for mail screening but also allow for advances that could be made to the technologies in future years.

The test piece is approximately A4-sized and is either run through the conveyorized X-ray machine or placed inside the cabinet compartment. The image obtained is assessed to determine the penetration and resolution performance of the system. Various image processing functions can be used to achieve the best possible image for assessment. The results of the image assessment should be recorded so that system performance can be compared over time and any degradation in performance is readily apparent.

It is important to note that interpretation of X-ray images requires specialist training.

UK Mail Screening Test Piece (MSTP) – A Guide is available on the CPNI website (www.cpni.gov.uk). The document gives a description of each individual test outlining the purpose of the test, its relevance to mail screening and the recommended performance standard. It is recommended that X-ray machines meet these standards as a minimum; systems that perform better than the minimum recommended standard offer greater performance capability for mail screening. Where organizations assess that they are at greater risk from attack through their mail streams, they can of course set their own internal performance standards. The guidance document also provides examples of log-sheets which offer a quick and easy method for recording results and comparing performance over time.

D.3 Threat image projection (TIP)

Threat image projection (TIP) has been used on conveyorized X-ray machines for aviation security applications for a number of years. This is where, periodically, the system projects an image of a threat object, for example, an explosive device or a knife, onto the X-ray image of the screened item. The operator has to detect the threat and press the designated button on the control panel to register that it has been seen. TIP is a well-established tool for X-ray detection systems, proven to aid motivation and performance monitoring in aviation security. It also provides images that are able to be used for training X-ray operators.

TIP products used in aviation security utilise a library of images of items considered to be a threat to aviation. Other generic threat image libraries are also marketed by X-ray equipment suppliers. Where TIP is used, it is important that the images are representative of threats relevant to the application. For example, using a TIP library designed for aviation security in a mail screening operation could undermine the operator's ability to detect certain postal threats.

A collection of items considered to be representative of a broad range of postal threats was developed by the Home Office Centre for Applied Science and Technology (CAST), in association with CPNI. Using these items, X-ray equipment manufacturers and suppliers have been able to develop TIP libraries for mail screening, with a number of such libraries now commercially available for use with conveyorized and cabinet X-ray systems.

Organizations might wish to consider the use of relevant TIP libraries for mail screening. TIP should improve the effectiveness of mail screening capability and the ability to quantify effectiveness. TIP also offers significant benefits as a tool to monitor operator performance, help maintain motivation and identify training needs.

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 16000, *Security management – Strategic and operational guidelines*

BS 31100, *Risk management – Code of practice*

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

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

Further reading and useful websites

Centre for the Protection of National Infrastructure

www.cpni.gov.uk

Contains guidance and information on a broad range of relevant topics, including threats to UK organizations, risk assessment, security planning, post rooms, personnel security, cyber security, CCTV systems and other physical protective measures.

National Counter Terrorism Security Office

www.gov.uk/nactso

Contains guidance and information on business security and resilience, and contact details for local Counter Terrorism Security Advisors.

Health and Safety Executive

www.hse.gov.uk

Contains guidance and information on dealing with suspect packages, particularly biological and chemical threats by post, personal protective equipment, risk assessment, and ionising radiation regulations.

In addition, the following relevant publications are available from the Health and Safety Executive:

Personal Protective Equipment at Work Regulations 1992. Guidance on Regulations (L25). HSE Books, 2005. ISBN 0 7176 6139 3.

Respiratory protective equipment at work: A practical guide. HSE Books, 2013. ISBN 978 0 7176 6454 2. This booklet provides information on the wide range of respiratory protective equipment available, including useful illustrations, and gives detailed advice on the selection of appropriate equipment. The importance of proper training and maintenance is emphasized.

Public Health England

www.gov.uk/government/organisations/public-health-england

Contains guidance and information on suspect packages and materials, risk assessment and radiation.

Register of Security Engineers and Specialists (RSES)

www.ice.org.uk/rses

The *Register of Security Engineers and Specialists (RSES)* is sponsored by CPNI and administered by the Institution of Civil Engineers (ICE). Individual Registrants are not listed in open source documentation. However, a client can verify that a Registered Security Engineer or Specialist is what they purport to be and in good standing by contacting the Institution via email to registers@ice.org.uk. The individual Registrant will be advised of the nature of the enquiry. A list of companies employing members of the RSES is also available from the RSES website. A list of competencies demonstrated by RSES members is also available from the RSES website.

Skills for Security

www.skillsforsecurity.org.uk

SFSMHS3:2014, *Screen mail*

Sets out the skills, knowledge and understanding for mail handlers to screen items of mail, including letters and parcels, delivered by hand, postal services and couriers, using technologies, techniques and processes.

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)20 8996 9001 Fax: +44 (0)20 8996 7001

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)20 8996 7669 Fax: +44 (0)20 8996 7001
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)20 8996 9001 Fax: +44 (0)20 8996 7001
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 Fax: +44 (0)20 8996 7005
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)20 8996 7002 Fax: +44 (0)20 8996 7001
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

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Department.

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

BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom

www.bsigroup.com

ISBN 978-058089-290-5