Introduction to **PAS 97**:2015

Mail screening and security – Specification

CPNI
Centre for the Protection
of National Infrastructure

bsi.

Introduction

PAS 97:2015 is a specification for mail screening and security within your organization. It contains everything you need to help identify and implement appropriate postal security and screening measures that address the risks your organization faces.

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.

PAS 97 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.

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

PAS 97:2015 was commissioned by the Centre for the Protection of National Infrastructure (CPNI), who provided the initial draft for development. Its production was facilitated by the British Standards Institution (BSI) with input from a panel of industry experts.

This booklet provides an introduction to PAS 97. The full version is available to order from **http://shop.bsigroup.com/pas97**.

Who is it for?

PAS 97 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.

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

- Understand the postal threat
- Understand the ways in which items of mail may cause concern, disruption, or harm
- Assess the extent to which the organization is a target

- Understand the organization's mail streams

Select _Screening Levels_ commensurate with the risk

Identify suitable location for screening facility and appropriate _Physical Protective Measures_

Formally record the organization's requirements for mail screening and security

Implement mail screening and security measures

- General postal security measures
- Management and responsibility
- Internal provision vs. outsourcing
- Operating procedures and emergency procedures

- Mail room location, design, layout and construction
- Screening methods and equipment
- Human factors
- Health and safety

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

Screening levels

A key component of PAS 97 is a series of screening levels.

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, whilst having 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.

What are discrete threat objects and "white powders"?

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

1. discrete threat objects and bulk materials;
2. "white powders".

Discrete threat objects and bulk materials 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.

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. Such materials may not be "white" and may not be "powders"; materials may be crystalline (e.g. sugar), oily or waxy residues, or liquids, and might be present in sufficiently small quantities as to be undetectable by typical X-ray-based screening processes.

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. PAS 97 provides actions that are recommended upon discovery of any suspicious delivered item.
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	

Protective measures

Once the different mail streams within the organization have been identified and assessed, and the appropriate screening levels assigned, the next step is to specify and implement the necessary screening and security measures and facilities.

Several classes of physical protection measures are detailed in PAS 97; these predominantly relate to the design,

construction (including ventilation) and layout of the mail room, but also include personal protective measures.

Recording the organization's requirements

It is important for the organization to 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. The information to be recorded includes:

✓ a summary of the organization's mail streams, including volumes and timing constraints;

✓ a summary of the threats the organization faces;

✓ 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.

It is also important that organizations consider postal security as an integral part of the wider security measures.

Implementation

Once the organization's requirements for mail security and screening capability have been formally stated, the various aspects of implementation can be addressed.

Many of the strands will be inter-related so it is important not to consider them in isolation.

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.

Further information provided in PAS 97

PAS 97 includes annexes as follows:

Annex A – Possible indicators that a delivered item may be of concern

Annex B – Action upon discovery of any suspicious delivered item

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

Annex D – Additional information on X-ray machines for mail screening

Bibliography

PAS 97 provides a comprehensive framework to help organizations identify and implement effective postal security measures to reduce their vulnerability to postal threats.

Acknowledgement

How to order a copy

Copies of PAS 97 can be purchased from **http://shop.bsigroup.com/pas97**