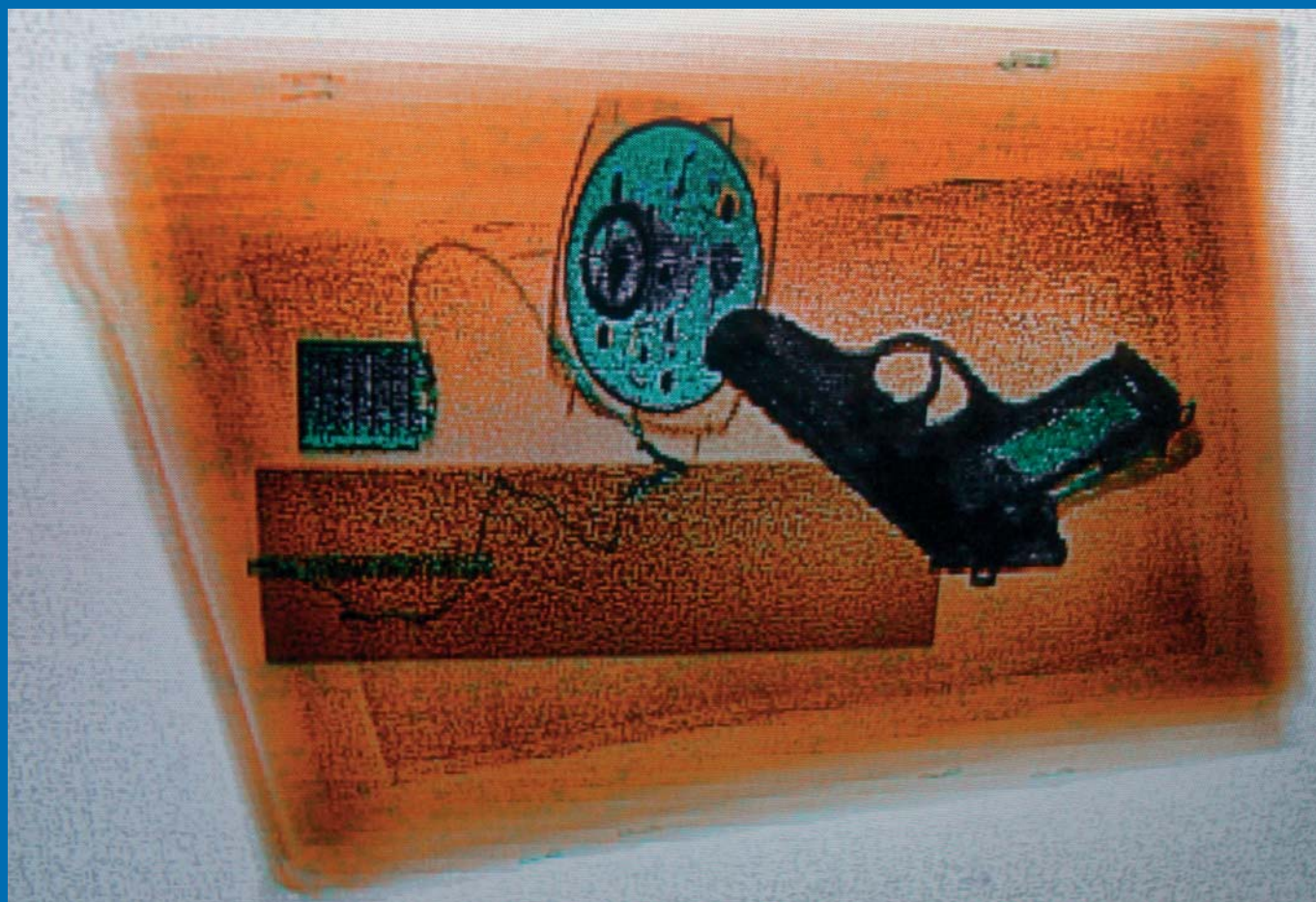


PAS 97:2009

A specification for mail screening and security



CPNI

Centre for the Protection
of National Infrastructure

ICS code: 13.310

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSi

British Standards
Documents

AVA

Document Sharing Hub

This Publicly Available Specification comes into effect on 31 March 2009

© BSI March 2009
ISBN 978 0 580 63094 1

Amd. No.	Date	Comments

Contents

Page

ii	Foreword
iii	Introduction
1	1 Scope
1	2 Terms and definitions
2	3 Outline of process
4	4 Assessing the risk
4	4.1 General
4	4.2 Understanding the threat
6	4.3 Understanding the organization's mail streams
8	5 Screening levels
8	5.1 General
8	5.2 Selecting appropriate screening levels for different mail streams
10	6 Physical protective measures
15	7 Summarizing the organization's requirements
16	8 Implementation
16	8.1 General
16	8.2 General postal security measures
16	8.3 Management and responsibility
18	8.4 Operating procedures (including emergency procedures)
19	8.5 Mail room / screening facility
20	8.6 Screening methods and equipment
21	8.7 Human factors
22	8.8 Health and safety considerations
23	Annexes
23	Annex A (informative) Sources of advice and information
24	Annex B (informative) Possible indicators that a delivered item may be of concern
25	Annex C (informative) Action upon discovery of any suspicious delivered item
26	Annex D (normative) Mail facility layout and construction to minimize the effects of an explosive device
31	Annex E (informative) Additional information on X-ray machines for mail screening

Foreword

This Publicly Available Specification (PAS) has been developed by the Centre for the Protection of National Infrastructure (CPNI) in collaboration with The British Standards Institution (BSI).

Acknowledgement is given to the following organizations that were instrumental in the development of this PAS:

- Arup Security Consulting
- BP
- G4S Cheltenham
- Home Office
- Mail Source UK
- MFD Group
- Palace of Westminster
- Pfizer
- Pitney Bowes
- Royal Mail
- Sister Banks Group

Acknowledgement is also given to the following organizations that were consulted in the development of this PAS:

- BBC
- British Forces Post Office
- Department for Business, Enterprise and Regulatory Reform (BERR)
- Driver and Vehicle Licensing Agency
- EDF Energy
- EON
- GCHQ
- Government Car and Dispatch Agency
- HM Revenue and Customs
- Metropolitan Police Service

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

In this PAS, the word “shall” indicates a requirement. The word “should” indicates a recommendation. Paragraphs marked “NOTE” are for guidance in understanding or clarifying the associated requirement.

This PAS has been prepared and published by BSI, which retains its ownership and copyright. BSI 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 does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

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

This PAS is not to be regarded as a British Standard.



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 may be intended to cause physical damage to property, harm to individuals, create fear or merely to cause disruption. 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 may 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 may 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.

Further sources of advice and information can be found in Annex A.

Case Study A

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 B

US Anthrax Letters, Autumn 2001

In September and October 2001, letters containing anthrax 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 may 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 C

UK Hoax Campaign, 2003 to 2007

A series of hoax "anthrax" letters were sent to high profile individuals throughout the UK between 2003 and 2007, as part of a wider campaign that also included letters containing racist threats. Dozens of mail items each containing small quantities of materials such as weed killer, salt, flour or sugar, typically wrapped in tin foil, were sent during this period. The amounts of materials were sufficiently small that they would most likely not have been discernable by bulk X-ray screening, though may have been detected by more intensive screening processes. Whilst the materials and quantities used proved relatively harmless, the campaign nonetheless caused significant concern and disruption.

Jefferson Azevedo, a postman from Portsmouth, was found guilty of offences contrary to the Anti-Terrorism Crime and Security Act 2001 and the Malicious Communications Act 1988, and sentenced to four years imprisonment.

Case Study D

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.

Case Study E

Business as Usual

A leading financial institution within the City of London employs a recognized contractor to conduct its mail handling and distribution, with approximately 70 staff employed across nine mail rooms. Both organizations recognize the benefit of robust screening processes as the financial implications of evacuating one of the institution's buildings in response to a mail room incident would be significant. To that end, they employ highly motivated and well-trained mail room staff, and place particular emphasis on continuation training.

Within the last five years there have been around 10 incidents where vigilant mail room staff have had cause to be concerned by particular packages, but by following the processes in place, have been able to confirm these as benign items of personal mail without adversely affecting the wider business.

1 Scope

This PAS gives requirements and recommendations for mail screening, set in the broader context of postal security. It is targeted at 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. 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. 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 purpose 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 may 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 will be used throughout this PAS (with postal used as the corresponding adjective).

2.3 mail handling

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



2.4 mail room

room or multi-room facility where mail is sorted and/or screened

2.5 mail screening

use of manual or automated methods to identify potential hazards and other causes of disruption associated with items of mail

2.6 mail streams

routes by which mail 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 enters, travels within, and exits the organization.

NOTE 2 Mail streams within the organization may span multiple sites or include off-site mail handling/screening by specialist contractors.

2.7 personnel security

measures used to confirm an individual's identity, qualifications, experience and right to work, and to monitor conduct as an employee or contractor

2.8 postal security

encompasses both mail screening and more general measures aimed at seeing all incoming, outgoing and internal mail streams are managed so as to minimize the risk of loss or theft

2.9 risk

reflects the impact and likelihood of an incident arising as a result of the threat

2.10 sensitive information

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

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

2.11 threat

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

2.12 "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. It 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 1 More general information on business risk management can be found in BS 31100, Risk Management, Code of practice and BS 25999, Business Continuity Management, as well as from the sources in Annex A.

Organizations demonstrating or requesting compliance with measures set out in this PAS shall do so using the format "PAS 97:2009 at screening level *n* with physical protection class *x*".

NOTE 2 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



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 impact and likelihood of an incident occurring.

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 may cause concern, disruption or harm, either unintentionally or as a result of malicious intent.

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.

Staff shall be trained to be aware of postal security issues and to be vigilant.

NOTE 2 A list of possible indicators that a delivered item may be of concern is presented in Annex B. This list is quite general, and what may be deemed suspicious in one context may be quite normal in another.

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.

The hazardous materials and items that could be contained in mail include:

- 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 materials (e.g. faeces, urine);
- Chemicals – toxic, corrosive or otherwise harmful, including narcotics;
- Biological materials;
- Radiological (radioactive) materials.

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" (see 2.12).

NOTE 3 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 4 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; suspected 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 discernable when mail is X-rayed, even if a large volume of mail is X-rayed at once.

This category includes:

- Explosive and incendiary devices;
- Firearms and ammunition;
- Knives;
- Blades;
- Most other sharp items;
- Offensive material (e.g. faeces, urine);
- Bulk chemical, biological and radiological 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 discernable in the X-ray image, provided the image is not too cluttered and the operator is well 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 may not be discernable when items of mail are X-rayed, especially when X-rayed in bulk. These materials may be dispersed within the envelope or package (so have no obvious shape, unless encouraged to aggregate in a corner as a result of gentle tapping); 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 may be a target. This analysis 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 may 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 may 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 may 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 analysis should include things the organization itself does or stands for, including sponsorship relationships; things other organizations in the same industry may 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) may 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 may 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) will 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 may warrant being subdivided for the purposes of this analysis. For example, items addressed to high profile individuals (by name or by position) or specific flag-ship addresses may be particularly likely to be targeted.

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

