PAS 29000:2021

Commercially operated vehicles – Framework for mitigating security risks from malicious use – Specification





Department for Transport

CPNI® Centre for the Protection of National Infrastructure

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2021.

ISBN 978 0 539 13445 2

ICS 03.220.20; 43.040; 43.120

Publication history

First published May 2021

Contents

Foreword

This PAS was sponsored by the Department for Transport (DfT) and 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. It came into effect on 31 May 2021.

Acknowledgement is given to Alexandra Luck, as the technical author, and the following organizations that were involved in the development of this PAS as members of the steering group:

- A Luck Associates
- AU Security Consulting
- Centre for the Protection of National Infrastructure (CPNI)
- Confederation of Passenger Transport UK (CPT)
- Construction Plant-Hire Association (CPA)
- Counter Terrorism Policing Headquarters (CTPHQ)
- Department for Transport (DfT)
- Fleet Operator Recognition Scheme (FORS)
- Hire Association Europe (HAE)
- Institute of Couriers (IOC)
- Logistics UK
- National Crime Agency (NCA)
- Road Haulage Association (RHA)
- Society of Motor Manufacturers and Traders (SMMT)
- The Office of the Traffic Commissioners
- Unite the Union

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

This PAS is not to be regarded as a British Standard. It will be withdrawn in the event it is superseded by a British Standard.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.

Information about this document

Certification. Users of PAS 29000 are advised to consider the desirability of third-party certification of conformity to this PAS. Users seeking assistance in identifying appropriate conformity assessment bodies or schemes may ask BSI to forward their enquiries to the relevant association.

This publication can be withdrawn, revised, partially superseded or superseded. Information regarding the status of this publication can be found in the Standards Catalogue on the BSI website at bsigroup.com/standards, or by contacting the Customer Services team.

Where websites and webpages have been cited, they are provided for ease of reference and are correct at the time of publication. The location of a webpage or website, or its contents, cannot be guaranteed.

Presentational conventions

The provisions of this PAS are presented in roman (i.e. upright) type. Its requirements are expressed in sentences in which the principal auxiliary verb is "shall".

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

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. "organization" rather than "organisation").

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Compliance with a Publicly Available Specification cannot confer immunity from legal obligations.

Introduction

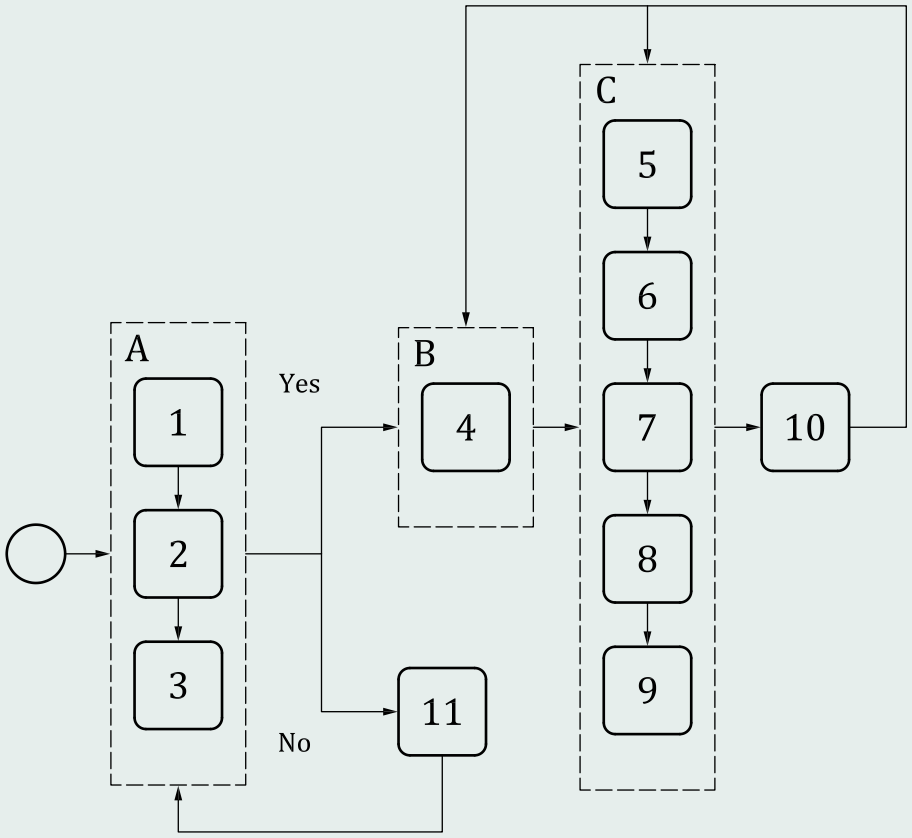
Events around the world have increased the awareness of the use of vehicles as a means to cause damage, to injure and kill. Vehicles have been used as a delivery mechanism for large explosive devices, known as a vehicle-borne improvised explosive device (VBIED) attack. Vehicles have also been used by themselves to breach a perimeter, ram and damage infrastructure, or as a weapon to injure and kill people, referred to as a "vehicle as a weapon" (VAW) attack. In other cases, vehicles have been used as a means to facilitate another action through deception or duress or in a combination of the actions described.

However, commercially operated vehicles are also used in other forms of serious and organized crime including drug operations and vehicle and cargo theft as well as undesirable actions such as anti-social behaviour. While these types of events do not generally receive the same level of attention as vehicles used in terrorist incidents do, they are more prevalent.

Both types of use can, directly or indirectly, cost society. It also has an impact on the organization that operates any vehicle used in an attempted or successful action, potentially causing damage to the organization itself, its function, assets, personnel and reputation.

This PAS sets out a process (see Figure 1) for the implementation of measures by organizations that are operators of commercial vehicles, whether these vehicles are owned by the organization, leased or hired from others, that aims to thwart both types of use. The approach described can be tailored to all organizations, whether large or small, and to ensure that the measures adopted by an organization are appropriate and proportionate to the security risks that arise from a threat actor obtaining and using one or more of its vehicles.

Figure 1 – Overview of the approach set out in this PAS



Key

A Establish the need for organizational counter measures to malicious use of commercially operated vehicles

B Initiate the approach to security of the organization's commercially operated vehicles

C Develop a security management plan

1 Obtain information on the risks

2 Assess the relevance of the risks in relation to the organization's vehicles

3 Determine the risks relative to the organization's risk appetite

4 Establish governance, accountability and responsibility for the security

5 Assess the specific security risks

6 Identify, assess and record existing security risk mitigation measures

7 Determine and develop any additional security risk mitigation measures

8 Develop policies and processes to implement mitigation measures

9 Develop a security breach/incident management plan

10 Monitor, audit and review

11 Review regularly or when a trigger event occurs

1 Scope

This PAS specifies requirements for the process of identifying, implementing and maintaining security measures to reduce the risk of commercially operated vehicles being used in acts of terrorism and other forms of serious and organized crime, including drug operations and vehicle and cargo theft as well as undesirable actions such as anti-social behaviour.

It covers personnel security and physical security of sites and vehicles as well as security management planning and processes.

The PAS is intended for operators of:

- light and heavy goods vehicles;
- public service vehicles (PSVs); and
- mobile plant,

whether they are leased, hired or owned by the operator or driver.

This PAS does not apply to organizations whose sole business relates to the hiring out of commercial vehicles, for example, members of the Rental Vehicle Security Scheme.

NOTE *Further information on the Rental Vehicle Security Scheme can be found on the Department for Transport website [1].*

This PAS is intended for use in the UK but, where appropriate, can be used in Europe or anywhere else in the world.

2 Normative references

There are no normative references in this PAS.

3 Terms, definitions and abbreviated terms

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

3.1 Terms and definitions

3.1.1 commercially operated vehicle

vehicle being operated for the purpose of transporting, buying, selling or exchanging of goods, services or anything of value

3.1.2 goods vehicle

motor vehicle with at least four wheels designed and constructed for the carriage of goods and/or any trailer that might be towed

3.1.3 mobile plant

machinery, appliance or other similar device that is able to move independently, and is used for the purpose of performing construction work on a construction site

3.1.4 need-to-know

legitimate requirement of a prospective recipient of information to know, to access, or to possess sensitive information

3.1.5 operator

individual or organization which uses, or is responsible for, vehicles in commercial activities

3.1.6 public service vehicle

motor vehicle (other than a tramcar) which, being a vehicle adapted to carry more than eight passengers, is used for carrying passengers for hire or reward or, being a vehicle not so adapted, is used for carrying passengers for hire or reward at separate fares in the course of a business of carrying passengers

[SOURCE: Public Passenger Vehicles Act 1981[2]]

3.1.7 residual risk

risk that remains after controls have been implemented

[SOURCE: BS EN ISO 16530-1:2017, **3.52**]

3.1.8 risk

effect of uncertainty on objectives

NOTE 1 *An effect is a deviation from the expected. It can be positive (sometimes expressed as opportunities), negative (sometimes expressed as threats) or both.*

NOTE 2 *Objectives can have different aspects and categories and can be applied at different levels.*

NOTE 3 *Risk is often characterized by reference to potential events, their consequences and their likelihood.*

[SOURCE: BS ISO 31000:2018, **3.1**]

3.1.9 risk appetite

amount and type of risk that an organization is willing to pursue or retain

[SOURCE: BS EN ISO 22300:2018, **3.202**]

3.1.10 security

state of relative freedom from threat or harm caused by deliberate, unwanted, hostile or malicious acts

3.1.11 security breach

infraction or violation of security

[SOURCE: BS ISO 14298:2013, **3.30**]

3.1.12 security culture

set of values, shared by everyone in an organization, that determine how people are expected to think about and approach security

3.1.13 security incident

suspicious act or circumstance threatening security

3.1.14 senior management

person or group of people who direct and control an organization at the highest level

NOTE 1 *Senior management has the power to delegate authority and provide resources within the organization.*

NOTE 2 *In the context of this document, management should be regarded as the function, not the activity.*

3.1.15 threat

potential cause of an incident which might result in a security breach

3.1.16 threat actor

person or entity that seeks to cause an incident which might result in a security breach

3.1.17 vulnerability

weakness in security that can be exploited by a threat actor

3.2 Abbreviated terms

ACT	Action Counters Terrorism
CTSA	Counter terrorism security advisor
VAW	vehicle as weapon
VBIED	vehicle-borne improvised explosive device

4 Establishing the need for organizational counter measures to malicious use of commercially operated vehicles

4.1 Undertaking a risk assessment process

The senior management of an organization that operates commercial vehicles, whether it owns them or leases or hires them from another organization, shall assess the need for organizational counter measures to malicious use or theft of commercially operated vehicles following the stages set out in **4.2** to **4.4**.

***NOTE** Wherever the term "organization" is used in the remainder of this document, it refers to the organizations referred to in **4.1**.*

4.2 Obtaining information on the risks

The senior management of the organization shall collate information on the range of security risks that arise from a threat actor obtaining a commercially operated vehicle(s):

a) to carry out a vehicle-borne attack; and

b) to facilitate other criminal actions.

***NOTE 1** Vehicle-borne threats range from vandalism to sophisticated or aggressive attack. A vehicle can be used as a delivery mechanism for a large explosive device [known as a vehicle-borne improvised explosive device (VBIED) attack], a vehicle by itself can also be used with hostile intent to breach a perimeter, ram and damage infrastructure, or as a weapon to injure and kill people [referred to as a "vehicle as a weapon" (VAW) attack], or it can be used as a means to facilitate another action through deception or duress. A vehicle can also be used in a combination of these measures.*

***NOTE 2** Attacks can be carried out by criminals and terrorists.*

***NOTE 3** A number of the measures set out in the document can be used to reduce the likelihood of vehicle theft where that theft does not result in a vehicle-borne threat.*

4.3 Assessing the relevance of the risks in relation to an organization's vehicles

The senior management of the organization shall, supported by competent risk manager(s), assess, taking into account the full threat picture current at the time, whether or not any of the vehicles that it operates might be of interest to a threat actor to carry out a vehicle-borne attack or for theft for other purposes.

***NOTE 1** Where there is insufficient knowledge or experience within the organization in relation to security risks, additional advice from competent external specialists should be obtained. Users of this PAS are advised to consider the Register of Security Engineers[1], the Register of Chartered Security Professionals[2] and the UK register of Independent Security Consultants.[3]*

***NOTE 2** Advice can be obtained from Counter Terrorism Security Advisers (CTSAs). CTSAs work with businesses to identify and assess sites that might be vulnerable to terrorist attack and advise them about counter terrorism protective security guidance that should be incorporated into their general crime prevention plans, advice and guidance. Further guidance is offered by the National Counter Terrorism Security Office [3].*

***NOTE 3** Specialist advice might also be available through relevant trade associations and business groups.*

***NOTE 4** Further guidance is provided by the Department for Transport [4], [5].*

4.4 Determining the risks relative to the organization's risk appetite

The senior management of the organization shall determine the organization's risk appetite and whether or not the use of one or more vehicles that it operates as part of a vehicle-borne attack exceeds it.

***NOTE 1** In addition to the potential harm caused to members of the public, the emergency services and other third parties, the use of an organization's vehicle in an attempted or successful attack can impact on the organization itself, its function, assets, personnel and reputation.*

***NOTE 2** Information on risk assessment can be found in BS ISO 31000.*

[1] See https://www.rses.org.uk
[2] See https://www.charteredsecurityprofessional.org
[3] See https://securityconsultants.org.uk

4.5 Recording the outcome

The organization shall record and retain each stage and the final outcome of the assessment process, including where the risk does not exceed the organization's risk appetite, and recognize that the outcome itself might be sensitive and on a need-to-know basis.

***NOTE** This record should be made within a reasonable timescale, taking into consideration the size of the organization, the level of risk, the risk appetite of the organization and the national threat level at the time.*

4.6 Reviewing the outcome of assessment process

4.6.1 The organization shall establish a mechanism for performing regular reviews at a minimum frequency of once every twelve months, as well as event-driven reviews, that check whether there is any change in the relevance of the risks in relation to the organization's vehicles or the organization's risk appetite.

4.6.2 The organization shall carry out a review if any of the following events occur:

a) a change in the type of commercial vehicles operated;

   ***NOTE 1** The vehicles now operated by the organization might be of more or less interest to a threat actor than those operated previously.*

b) a change in the security context;

   ***NOTE 2** A change in the security context includes a change in the threats that exist or the techniques that a threat actor might use.*

c) a significant change in the existing site where vehicles and/or goods or other products are stored;

   ***NOTE 3** A significant change in the site includes a change in the perimeter of the site or a change in the use of the land surrounding the perimeter of the site.*

d) the creation of a new site for the storage of vehicles; or

e) when events occur that reveal vulnerabilities not previously anticipated.

   ***NOTE 4** An event such as a security breach or incident, including a disrupted or thwarted security breach/incident should trigger a review of the outcome of the assessment process.*

4.7 Risks identified

Where the outcome of the assessment process is that the risk exceeds the organization's risk appetite, the organization shall, following the requirements of this document, develop and implement an appropriate and proportionate security management plan.

***NOTE** A proportionate security management plan is one that is pragmatic, appropriate and cost effective. A security management plan that is proportionate for a large organization might not be proportionate for a much smaller one. However, an organization, regardless of how large or small it is, might also operate some vehicles that are of greater potential interest to a threat actor and therefore might need to apply different measures to those applied by an organization that operates vehicles which could be of less interest.*

4.8 Negligible risks identified

4.8.1 Where the outcome of the assessment process, taking into account the full threat picture current at the time, is that the risk does not exceed the organization's risk appetite, the organization shall assess whether there are any other benefits to be derived from implementing a security management plan.

4.8.2 The organization shall continue to monitor the outcome of the assessment process as set out in **4.6**.

***NOTE** Unless the organization wishes to implement a security management plan for other reasons, there is no necessity for the requirements of Clause **5** to Clause **12** to be applied.*

5 Initiating the approach to security of the organization's commercially operated vehicles

5.1 The senior management of the organization shall establish governance, accountability and responsibility for security.

5.2 The senior management of the organization shall define the individual at senior management level accountable for the approach to security to be adopted.

5.3 The organization shall define the individual(s) responsible for:

a) identifying the security threats and vulnerabilities associated with the potential malicious use of the organization's commercially operated vehicles;

b) developing the security management plan or, where the organization already has a security management plan, managing the embedding of a record of the additional security risks and mitigation measures arising from following the requirements of this document;

c) offering guidance and direction on the handling of the resultant security risks;

d) assessing the organization's existing security measures in place and their suitability to mitigate the security risks identified;

e) managing the implementation of the security management plan;

f) advising on the need for, and undertaking, the reviewing and auditing of security risk mitigation measures implemented;

g) advising on the need for, and where appropriate, undertaking or commissioning, testing of the relevant security measures;

h) managing the organization's response to any security breaches and incidents, including disrupted or thwarted security breaches/incidents;

i) reviewing the organization's security management plan; and

j) where required, seeking advice from appropriate security experts who can demonstrate competence in the required areas.

NOTE *Information on possible sources of advice are contained in* ***4.2****, Notes 1 to 3.*

5.4 The organization's governance, accountability and responsibility arrangements shall be recorded and retained as part of the security management plan.

6 Developing a security management plan

6.1 The organization shall develop a security management plan which includes:

a) a record of the outcome of the assessment process set out in Clause **4**;

b) the governance, accountability and responsibility arrangements for the security approach (see Clause **5**);

c) an assessment of the specific security risks to the organization in relation to the commercially operated vehicles it operates (see Clause **7**);

d) the security risk mitigation measures currently in place (see Clause **8**);

e) an assessment of potential additional security mitigation measures (see **9.1** to **9.4**)

f) the mitigation measures to be implemented (see **9.5**);

g) a summary of the tolerated security risks and residual tolerated security risks (see **9.6**);

h) the policies and processes for implementing the security mitigation measures (see **9.7**);

i) the arrangements for monitoring and auditing the mitigation measures implemented (see Clause **10**);

j) the arrangement for managing security breaches and incidents (see Clause **11**); and

k) the arrangements for reviewing and updating the security management plan (see Clause **12**).

6.2 Where the operator hires in commercial vehicles from third-party rental companies, the security management plan shall set out the specific advice on the security provisions that shall be instigated.

6.3 Access to any part of the assessment process, which details the security risks identified, shall be managed on a strict need-to-know basis. All such information shall be subject to security measures appropriate to the level of risk with regard to its creation, distribution, use, storage, disposal and destruction.

NOTE *The security management plan should be developed and implemented within a reasonable timescale of the need being identified, taking into consideration the size of the organization, the level of risk, the risk appetite of the organization and the national threat level at the time.*

7 Assessing the specific security risks

The organization shall assess the specific security risks related to its commercially operated vehicles by determining:

a) the potential threat actors who might seek to obtain, for malicious use, the commercial vehicles the organization operates;

b) the potential vulnerabilities that exist in relation to its site(s) and the commercial vehicles it operates, both when on the organization's site(s) and at other locations;

NOTE 1 *Vehicles might be parked at other locations overnight and when not in use, for example, at construction sites, in third-party compounds or in dedicated parking areas adjacent to, or remote from, the highway.*

c) the nature of the harm which can be caused, by the use of one or more of the commercial vehicles that it operates in an attempted or successful attack, to members of the public, the emergency services and other third parties, the organization itself, its function, assets, personnel and reputation;

d) the likelihood of a vehicle that the organization operates being of interest to a threat actor to carry out a vehicle-borne attack, including a VAW or VBIED attack, as a means to facilitate another action through deception or duress, or to be stolen for another type of criminal action; and

NOTE 2 *More information on types of vehicle-borne attacks is contained in* ***4.2****, Notes 1 and 2.*

e) the resultant risks by analysing the combinations of impact and likelihood.

NOTE 3 *In assessing the security risks, it can be appropriate to use the same risk scoring approach in place elsewhere in the organization.*

8 Identifying, assessing and recording existing security risk mitigation measures

8.1 The organization shall identify and document any security measures already in place.

8.2 The organization shall document the risk reduction achieved by these measures in relation to the outcome of the assessment of the specific security risks related to the commercial vehicles it operates.

8.3 The organization shall determine where a level of security risk that exceeds the organization's risk appetite remains.

8.4 Where the level of security risk exceeds the risk appetite of the organization, the organization shall develop and implement security risk mitigation measures to address these in accordance with the requirements set out in Clause **9**.

9 Determining and developing any additional security risk mitigation measures required

9.1 Assess potential additional security risk mitigation measures

By examining the measures set out in **9.2** to **9.4**, the organization shall assess the potential additional personnel, physical and cyber security risk mitigation measures it could implement.

NOTE 1 *The interplay between personnel and physical controls, as well as cyber and technical aspects of physical systems, can be exploited by threat actors if the links across these areas have not been examined.*

NOTE 2 *Guidance on cyber security measures is available from www.ncsc.gov.uk/section/advice-guidance/all-topics [6].*

9.2 People, security culture and behaviours

9.2.1 The organization shall take into account its workforce, contractors (including the supply chain), agency staff and visitors in the personnel security measures that it develops.

9.2.2 In assessing the need for any additional security measures in relation to personnel security, the organization shall implement, or document its justification for not implementing:

NOTE 1 *Further guidance on a) to f) below is provided by the Department for Transport [4], [5].*

a) robust pre-employment checks for all employees;

NOTE 2 *Robust pre-employment checks for all employees can help mitigate the insider threat deterring applicants who might wish to harm the organization from applying for employment and detecting individuals with an intent to harm the organization at the recruitment/application phase.*

NOTE 3 *Consideration should be given to using BS 7858 for security screening of employees. This standard involves conducting basic identity, financial, employment and criminal records checks.*

NOTE 4 *When employing drivers, users of this PAS are advised to consider the following additional steps:*

1) *checking a driver's references and previous employment history for a minimum of the previous five years;*
2) *gaining references from previous employers;*
3) *informing applicants that false details on application forms can lead to dismissal;*
4) *checking driving licences are valid and looking for endorsements before employing someone, followed by checks at six-monthly intervals afterwards;*
5) *requiring drivers to inform the organization of any changes to their licence;*
6) *checking whether the applicant has any prosecutions pending or is waiting for sentencing by a court;*
7) *for agency drivers, checking that the agency has carried out all of the checks listed in a) to f) including a criminal records check; and*
8) *only using recruitment agencies that are affiliated with a recognized UK trade organization.*

b) induction of all new personnel so that they are briefed on their responsibilities and the required security culture, including:

1) the need to provide and record general security awareness training alongside health and safety, and other similar training; and
2) a documented process for inducting all new staff including topics to be covered by these awareness sessions and the required learning outcomes from each;

NOTE 5 *The content of the security inductions should be related to the security risks identified and the security mitigation measures implemented by the organization.*

NOTE 6 *Training materials such as ACT awareness e-learning [7] and "Run Hide Tell" material [8] can be obtained from organizations including the National Counter Terrorism Security Office.*

c) security awareness and training requirements to develop and promote a security culture including refresher training;

NOTE 7 A strong security culture can promote positive security behaviours across the workforce.

NOTE 8 An effective security culture results in:

1) *awareness of the most relevant security threats;*
2) *increased compliance with protective security measures;*
3) *a workforce that is more likely to be engaged with, and take responsibility for, security issues;*
4) *a workforce that is more likely to think and act in a security-conscious manner; and*
5) *a reduced risk of insider incidents.*

NOTE 9 Guidance on developing a security culture is available on the Centre for the Protection of National Infrastructure (CPNI) website [9].

NOTE 10 The content of security awareness and training sessions should be related to the security risks identified and the security mitigation measures implemented by the organization.

d) role-based security training requirements to facilitate the adoption and maintenance of a security culture;

NOTE 11 Some roles, for example, those controlling access to sites, are likely to require specific training which can include detecting hostile reconnaissance, performing security checks and responding to vehicle theft attempts.

e) a means for staff to report security concerns or suspicions, either anonymously or otherwise; and

NOTE 12 A system for staff to report security concerns should be readily accessible to all staff and should be routinely monitored so that any issues are quickly identified, and any mitigation measures required, implemented.

f) measures to be taken when personnel leave the organization.

NOTE 13 When a member of personnel leaves the organization the processes in place should ensure that access to sites, vehicles and systems is removed, any electronic devices belonging to the organization and passes are returned.

NOTE 14 These measures should apply to both personnel who are members of staff and to contractors.

9.3 Physical security of sites

In assessing the need for additional security measures in relation to the physical security of operating centres and maintenance facilities, the organization shall implement, or document its justification for not implementing:

NOTE 1 Further guidance on a) to f) below is provided by the Department for Transport [4], [5].

a) creation of controlled environments which act as a deterrent and protect from theft and other criminal activity;

NOTE 2 Examples of site security measures that help create a controlled environment include:

1) *illumination of the area where vehicles are parked, including the perimeter and access routes;*
2) *fitting locks or tamper-proof seals to lockers and equipment boxes;*
3) *controlling access to operating centres with appropriate security arrangements, i.e. fences, gates, security codes; and*
4) *storing vehicle keys in a secure locker with security codes rather than leaving them in vehicles or on hooks in the office easily accessible to anyone.*

b) management of visitor and contractor access;

NOTE 3 Policies which should be considered include requiring:

1) *pre-booking of all visitors in advance of their arrival;*
2) *all visitors to report to reception or an individual in authority on arrival;*
3) *visitors to sign in and out of the site;*
4) *passes to be issued to all visitors which should be worn and visible;*
5) *challenge of any visitors not wearing a pass where such action does not compromise the individual's own safety;*
6) *visitors to be escorted at all times when not in public areas; and*
7) *a security awareness briefing to be given to all visitors.*

NOTE 4 Security briefings of visitors should include:

1) *requirement for wearing a pass while on site;*
2) *requirement for displaying any work/parking permits in the windscreen of any visitor vehicle parked on site;*
3) *the need to be vigilant when on the premises and the actions to take if they see a suspicious item or a person acting unusually;*

4) *the need to properly close all doors when leaving, particularly doors leading to non-public areas;*
5) *requirement for visitors not to tailgate into non-public areas; and*
6) *requirement, on leaving, to secure any equipment or any unoccupied area of the site to which the visitor has had access.*

c) control of vehicle access to sites;

NOTE 5 *The movement of any third-party vehicles on site should be strictly controlled and ideally prevented.*

d) security controls for areas where vehicles are parked when not in use;

NOTE 6 *Physical security measures that should be considered at sites where the organization's commercial vehicles are parked when not in use include:*

1) *access barriers around the site such as walls or fences;*
2) *access control measures at all entrances;*
3) *measures to protect vehicles on site, for example, locking of vehicles, regular patrols, and video surveillance systems (commonly called CCTV); and*
4) *not parking/placing any vehicles, trailers, equipment or materials near, or against, fences, gates or walls where they could be accessed or used as climbing aids.*

e) whether vehicles are maintained at off-site facilities, the security controls required at these facilities; and

NOTE 7 *The security controls should, where possible, be commensurate with those in place at the organization's own site(s).*

NOTE 8 *The maintenance agreement between the vehicle operator and the vehicle maintenance company should include a duty to secure the vehicles and keys correctly.*

f) site monitoring.

NOTE 9 *Users of this PAS are advised to consider using an electronic detection system listed on the CPNI Catalogue of Security Equipment.*

NOTE 10 *It is good policy that video surveillance systems are viewed once every five minutes. This aims to limit the potential time for an unauthorized activity to be undertaken and forces an attacker to act rapidly, increasing the likelihood that they will trigger an electronic detection system.*

NOTE 11 *Guidance on the provision of physical security measures, including barriers, is contained on the CPNI website [10].*

NOTE 12 *Effective security measures at operating centres and maintenance facilities can help to create a controlled environment which will encourage positive security behaviours amongst staff, act as a deterrent and protect from theft and other criminal activity.*

9.4 Physical security of vehicles

In assessing the need for additional security measures in relation to the physical security of vehicles, the organization shall implement, or document its justification for not implementing:

NOTE 1 *Further guidance on a) to f) below is provided by the Department for Transport [4], [5].*

a) checks of vehicles when preparing to depart from their origin or following a stop;

NOTE 2 *Checks should include visual checks for damage, tampering and general road worthiness, as well as cab and cargo security.*

NOTE 3 *Even if a driver performs checks of a vehicle it is possible that they might fail to detect something that has been planted or stowed on the vehicle.*

b) the securing of vehicles that are left unattended, including when parked in an unsecure location;

NOTE 4 *The measures which the organization should consider implementing include requirements:*

1) *that vehicles should not be left unattended at the roadside with the engines running;*
2) *that ignition keys should not be left in the vehicle whilst the driver is not present;*
3) *regarding key control when the vehicle is not at the depot;*
4) *that all locks, alarms or other devices are engaged before the driver leaves the vehicle;*
5) *that operators of vehicles that require the engine to be running in order to operate auxiliary equipment, or heating or cooling systems in passenger carrying vehicles, when the driver is not in the cab, take appropriate measures to protect against theft of the vehicle, for example, the provision of a second key to lock the cab doors and the fitting of run lock type devices, which switch the engine off if attempts are made to drive off by unauthorized drivers;*
6) *that vehicles are parked as securely as possible;*
7) *that drivers and/or goods vehicle operators should report any concerns about unusual behaviour that occurs on or close to their vehicle; and*

8) *that vehicles that do not require an ignition key to start should be fitted with additional security devices that only allow an authorized person to start the engine. Where keyless start or keyless entry and start exist, an additional immobilizer should be considered.*

c) measures to protect the security of the driver while the vehicle is in motion;

d) the requirements, where applicable, relating to vehicles permitted to carry members of the public;

NOTE 5 *Consideration should be given to:*

1) *only allowing passengers to board when the driver is present, after any luggage has been loaded, where applicable, and after a vehicle security check has been completed; and*

2) *a process by which the driver is able to satisfy themselves that the correct passengers are re-boarding if the vehicle makes a stop en-route (e.g. at a service station), for example, by asking the passengers to re-present their tickets.*

e) the safety and security equipment that should be fitted to different vehicles;

NOTE 6 *Safety and security equipment includes light goods vehicle load area security, slam locks, deadlocks, armoured locks and lock protection plates for when vehicles are not in use, and vehicle tracking systems, motion sensor alarm systems, and e-locks to alert drivers to unauthorized load area access and "jump up thefts" when vehicles are in use.*

NOTE 7 *Consideration should also be given to load compartment or on-vehicle CCTV and panic button type systems.*

NOTE 8 *Where there is a separate drivers' cab on vehicles permitted to carry members of the public, this area should have the provision to be made secure.*

f) the fitting and testing requirements for safety and security equipment fitted to vehicles to ensure they are fit for purpose;

NOTE 9 *All safety and security equipment should be fitted by a competent installer.*

g) the training of drivers on the use of, and familiarization with, the security equipment on-board any of the organization's vehicles they drive; and

h) the actions to be taken prior to the disposal of vehicle.

NOTE 10 *Removal of all company branding, including liveries and distinctive colour schemes, from the vehicle prior to disposal minimizes the risk that it could successfully be used to conduct a trojan attack.*

9.5 Determining mitigation measures to be implemented

9.5.1 The organization shall assess the potential mitigation measures, taking into account:

a) the cost of the mitigation measure and its implementation;

b) the risk reduction that can be achieved and level of residual risk;

c) the predicted cost impact of the mitigation measure;

NOTE 1 *A mitigation measure can result in additional costs to an organization beyond the cost of implementing the measure itself, it can also result in lower costs to, for example, insurance.*

d) the likelihood of the mitigation measure being used by personnel and embedded into the organization as business as usual;

NOTE 2 *The likelihood of a measure being used by personnel and embedded into the organization as business as usual determines how likely it is for the measure to successfully mitigate the identified security risk.*

e) other impacts that the mitigation measure can have on the asset;

NOTE 3 *This can include usability, efficiency and appearance.*

f) the potential for the measure to create further vulnerabilities; and

g) whether the measure delivers any other business benefits.

NOTE 4 *Business benefits can include reducing overall business risk and can extend to the organization and its staff better understanding the value of the organization's physical assets as well as its reputation.*

9.5.2 The organization shall use the outcome of the assessment to determine which mitigation measures, if any, are put in place.

NOTE *A proportionate mitigation measure is one that is pragmatic, appropriate and cost effective.*

9.6 Documenting residual and tolerated security risks

9.6.1 Following the development of any new security mitigation measures, the organization shall identify and record any residual security risks.

9.6.2 The organization shall continue the processes of assessing the security risk and developing security risk mitigation measures on these security risks until a point is reached where the organization's risk appetite is not exceeded.

9.6.3 The organization shall document the tolerated security risks.

9.7 Develop polices and processes to implement mitigation measures

9.7.1 The organization shall develop the policies and processes which enable the agreed mitigation measures to be implemented in a consistent manner.

9.7.2 The organization shall communicate, and make available, these policies and processes to staff and any relevant third parties.

9.7.3 The organization shall provide, and record the occurrence of, training, coaching and support to its staff, and any other relevant third parties, to facilitate understanding and consistent implementation of the security policies and processes.

10 Monitoring and auditing

10.1 The security management plan shall set out the appropriate and proportionate monitoring, auditing and testing measures which shall include assessing, at a minimum frequency of once a year, the implementation of all aspects of the security management plan.

10.2 The security management plan shall require that only competent individuals, as defined by the operator, shall undertake this monitoring and auditing work.

11 Responding to security breaches and incidents

11.1 General

11.1.1 The organization shall create and maintain a security breach/incident management plan as part of the security management plan which shall include:

a) an assessment of the types of security breaches/incidents that can occur and the potential risks that can arise;

b) the process to be followed on discovery of a security breach/incident, including a disrupted or thwarted breach/incident (see **11.2**);

__NOTE__ This should include the actions to be taken if an unattended item, or suspicious individual not recognized, is found in or around a vehicle.

c) the collection of evidence, where applicable, for law enforcement purposes (see **11.3**); and

d) the review process to be carried out following a security breach or incident, including the mechanisms for reviewing and updating the security breach/incident management plan (see **11.4**).

11.1.2 Parts of the security breach/incident management can be covered by other existing plans or national-specific actions and where this is the case, these plans or actions shall be cross-referenced.

11.1.3 The part of the security breach/incident management plan that records the risks shall be managed on a strict need-to-know basis with the information contained within those parts subject to appropriate security measures with regard to their creation, distribution, use, storage, disposal and destruction.

11.2 Discovery of a security breach or incident

11.2.1 The organization shall document the steps to be taken in the event of a discovery of a security breach or incident, including a disrupted or thwarted breach/incident, which shall include:

a) the persons or roles to be contacted immediately and their contact details;

b) the circumstances under which a collection of evidence for law enforcement purposes is required and the approach to be taken to preserve that evidence; and

c) handling any third-party, regulator, media or public interest in the event of a security breach/incident.

11.3 Containment and recovery

11.3.1 The organization shall document the steps to be taken in the event of a security breach/incident to contain and recover from the event that include an assessment of what has been lost, compromised or damaged.

11.3.2 Under circumstances where it is necessary to collect evidence for law enforcement purposes, all evidence (i.e. both physical and digital) that can aid an investigation to identify the perpetrators, shall be retained, preserved and collected, by the appropriate law enforcement agency, before any recovery actions are taken, unless the immediate need for such actions is critical to life.

__NOTE__ Potential evidence should be isolated and access made available to law enforcement to recover that evidence before any recovery actions are taken.

11.4 Review following a security breach or incident

11.4.1 Following the initial containment and recovery actions, the organization shall undertake an assessment of the ongoing risk. This assessment shall examine what facilitated the incident and identify potential countermeasures.

__NOTE 1__ Where there is insufficient knowledge or experience within the organization to conduct this review, additional advice from external specialists should be obtained.

*__NOTE 2__ Information on possible sources of advice are contained in **4.3**, Notes 1 to 3.*

11.4.2 The relevant policies and processes in the security management plan shall be updated to reflect the findings of the assessment and to prevent or reduce the risk of a re-occurrence.

12 Reviewing the security management plan

12.1 The organization shall establish a mechanism for performing periodic and event-driven reviews of the security management plan, including the effectiveness of the mitigation measures in place, to check that it remains fit for purpose.

12.2 Event-driven reviews shall be undertaken when political, social, organizational, technological, legal or environmental changes occur that can significantly impact on the organization or its commercially operated vehicles, or events occur that reveal vulnerabilities not previously anticipated.

NOTE *These include the types of situations described in* ***4.6****.*

12.3 A periodic review shall be undertaken, at a minimum, once every twelve months.

12.4 Following a review, the security management plan shall be updated to reflect any changes to the threats, vulnerabilities, resultant security risks and/or security risk mitigation measures.

12.5 The occurrence of each review and the reason for it being undertaken shall be recorded and retained as part of the security management plan.

12.6 Access to any part of the review that details the security risks identified shall be managed on a strict need-to-know basis, with all such information subject to security measures, appropriate to the level of risk, with regard to its creation, distribution, use, storage, disposal and destruction.

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 7858, *Screening of individuals working in a secure environment – Code of practice*

BS EN ISO 16530:2017, *Petroleum and natural gas industries – Well integrity – Part 1: Life cycle governance*

BS EN ISO 22300:2018, *Security and resilience – Vocabulary*

BS ISO 14298:2013, *Graphic technology – Management of security printing processes*

BS ISO 31000:2018, *Risk management – Guidelines*

Other publications

[1] DEPARTMENT FOR TRANSPORT. *Apply to the rental vehicle security scheme.* London: DfT, 2018. Available from: https://www.gov.uk/government/publications/apply-to-the-rental-vehicle-security-scheme

[2] GREAT BRITAIN. Public Passenger Vehicles Act 1981. London: The Stationery Office.

[3] NATIONAL COUNTER TERRORISM SECURITY OFFICE. *Working with counter terrorism security advisers*. London: NCTSO, July 2020. Available from: https://www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities/working-with-counter-terrorism-security-advisers

[4] DEPARTMENT FOR TRANSPORT. *Security guidance for goods vehicle operators and drivers*. London: DfT, 2019. Available from: https://www.gov.uk/government/publications/security-guidance-for-goods-vehicle-operators-and-drivers

[5] DEPARTMENT FOR TRANSPORT. *Bus and coach security: best practice*. London: DfT, 2018. Available from: https://www.gov.uk/government/publications/bus-and-coach-security-recommended-best-practice

[6] NATIONAL CYBER SECURITY CENTRE. *Advice & guidance*. London: NCSC, 2020. Available from: https://www.ncsc.gov.uk/section/advice-guidance/all-topics

[7] NATIONAL COUNTER TERRORISM SECURITY OFFICE. *ACT Awareness eLearning*. London: NCTSO, 2020. Available from: https://www.gov.uk/government/news/act-awareness-elearning

[8] NATIONAL COUNTER TERRORISM SECURITY OFFICE. *Stay Safe Film*. London: NCTSO, 2020. Available from: https://www.gov.uk/government/publications/stay-safe-film

[9] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Developing a security culture*. London: CPNI, 2020. Available from: https://www.cpni.gov.uk/developing-security-culture

[10] CENTRE FOR THE PROTECTION OF NATIONAL INFRASTRUCTURE. *Physical Security*. London: CPNI, 2020. Available from: https://www.cpni.gov.uk/physical-security

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

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

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards-based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email cservices@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Relations
Tel: +44 345 086 9001
Email: cservices@bsigroup.com

Subscription Support
Tel: +44 345 086 9001
Email: subscription.support@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

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

ISBN 978-0-539-13445-2