Risk Consulting RCG401

Security

Introduction

To prevent intruders such as thieves, vandals and arsonists from gaining access to any premises, suitable security measures are essential. Some intruders will be opportunistic, but others are determined and organised intruders who will have done their homework in targeting the “weakest link in the chain”. This is why a “layered protection” approach is often the best approach to achieve a level of security commensurate with the risk.

This guide focuses on perimeter and building security. It makes reference to guidance and best practice published within the United Kingdom, though most is applicable worldwide.

Essential Principles for Security of Property and Assets

Security measures can be considered in terms of three broad categories:

- Physical security
- Electronic security
- Human security

Some key points to remember when assessing or considering security measures are:

- Use specialist installers who are certified and approved by the organisations such as (in the UK) National Security Inspectorate (NSI) or The Security Systems Alarms Inspection Board (SSAIB). They will install and maintain in accordance with the appropriate standard and with the manufacturer’s guidelines
- Integrate security measures so that they work together. This includes integration with fire, health and safety measures, as well as cyber security measures
- Ensure that security measures are proportionate to the risk
- Ensure that security measures are managed and maintained regularly
- Ensure that staff are trained in the use of security systems and know how to respond to activations or breakdowns

There are a number of freely available documents on the RISCAuthority website (click on the Documents Tab) that cover all aspects of security management and controls.

Document Number: RCG401 v3 Date: 01/2025

Security Fencing

As well as defining a boundary, security fencing serves many purposes such as providing a deterrent and adding delays to potential intruders. They are particularly useful when used in conjunction with guards, security lighting and video surveillance making it a very useful first line of defence.

Certified companies will be able to install fencing to the relevant British Standard listed at the end of this guidance.

Maintenance of security fencing is very important, and procedures should be in place whereby the fence is inspected in its entirety on a regular basis, according to the degree of risk.

Any breaks, holes or other damage should be repaired without delay. Wherever possible, trees and undergrowth should not be permitted to grow close to the fence (on either side) as these can provide concealment and possibly be an aid to scaling the fence. For the same reasons, pallets, lighting/camera masts, material storage, outbuildings, skips, etc. should not be positioned close to a security fence.

Gates in security fencing should be installed to the same standard of security as the fence itself. In particular they should have no gaps or climbing aids that could be exploited by intruders.

The hinge pins of security gates may need to be capped by a disc of mild steel welded to the top of the pin to prevent the gates being lifted off their hinges, and good quality close shackle padlocks should be used to secure gates.

Alarm signalling can also be fitted to fences, though this must be done with care to avoid false alarms - see later for more on intruder alarms.

Closed Circuit Television (CCTV) / Video Surveillance Systems (VSS)

The presence of a VSS is widely accepted as a useful means to deter, or otherwise help to detect and limit, unauthorised access and criminal activity.

There are many types of systems available. Whatever type of system is used, it is important that it is reliable, resilient against interference and has the appropriate coverage. All ‘at risk’ areas should be covered e.g. entry points, approach routes and areas attractive to trespassers/criminals (much of the perimeter will be a target for entry points too). A suitable method of detector activation, ‘real time’ monitoring and response to viewed events is also essential.

Detector activated systems monitored at an approved remote video or alarm receiving centre, allow intrusion to be detected and observed remotely without the need for continuous on-site monitoring. In addition, such systems allow for live audible warnings to be issued to intruders. They should be integrated with intruder alarm systems so that they both cover 'at risk areas' and potential entry points.

NSI or SSAIB certified companies (or their equivalents in other countries) will be able to install a VSS to the relevant Standard (listed at the end of this guidance) and in accordance with manufacturer guidance. They will also be well placed to advise on placement and operation. Prior to the installation of a VSS, careful analysis should be made in consultation with insurers.

Doors

Entry/exit doors, especially those of lighter construction, can be vulnerable to attack by intruders even when they are fitted with the best quality locks and bolts. Door panels can be kicked in or hand-tools used to cut a body sized hole.

Even doors that appear solid are frequently found upon close inspection to be of only semi-solid construction and/or filled with lightweight material.

Many doors are not made from timber but are glazed within a frame, purpose-built uPVC doors or steel doors. Factors to consider are:

- The door should be robust and within an equally robust frame
- Timber doors should be of solid core and a minimum thickness of 45mm, noting that hardwood is generally stronger than softwood.
- Doors should be professionally installed
- Where the door provides direct access to theft attractive assets, they may need to be reinforced, especially if doors are glazed
- In all cases they should be fitted with alarm sensors, with further detection beyond the door (see alarms section later)
- The door should be fitted with BSI approved deadlocks, preferably 2 at the 1/3 and 2/3 positions.
- Where hinges are exposed, the door can have hinge bolts fitted to protect the hinge side of the door

Where reinforcement is required, the following specification may be suitable:

- Doors to be clad on their external face with a single panel of sheet steel not less than 1.5mm fixed using coach-bolts of a minimum diameter of 6mm passing through the full thickness of the door and spaced at intervals not exceeding 150mm, all round the perimeter of the door

- Coach-bolts to be fitted at similar intervals through the cross bracing and centre rails of the door
- All securing nuts and washers to be on the inside of the door welded to the bolts, or alternatively the ends of the bolts should be modified (burred) so they can't be readily undone
- If in exceptional circumstances, it is necessary to steel-reinforce the door on its internal face, 5.5mm diameter wood screws with non-return heads and at least 25mm in length should be used at intervals not exceeding 100mm in place of coach-bolts
- Hinge bolts should be installed top and bottom. In order to carry the additional weight, it may be necessary to fit additional hinges to the door

A common alternative is to install internal or external lockable steel bar/mesh gates, roller shutters, or internal collapsible (folding) steel grilles. These should be professionally fitted and ideally be certified as meeting a recognised security standard (see the list at the end of this guidance).

Windows

Many intruders will favour access via a window to gain unlawful entry.

Window locks offer a minimum level of protection that may be sufficient to deter an inexperienced opportunist, but they will not withstand a determined attempt at forced entry. Levering a window frame with a hand tool, or simply breaking and removing a glass pane will generally be sufficient to gain access.

It can therefore be desirable to ensure that glass is toughened or laminated, and/or to fit steel bar grilles to windows, particularly those in accessible and vulnerable locations such as the ground floor or upper floor emergency exits.

The following specification is suitable for locksmiths or builders when installing window grille bars:

- Grilles to comprise vertical solid steel bars at least 20mm in diameter or square section spaced at not more than 100mm centres. The bars to pass through and be welded to tie bars of flat steel not less than 35mm x 6mm spaced not more than 600mm apart
- Grilles to be fixed, preferably on the inside of a window opening, using one of the following methods:
  - Bars to be grouted into the brickwork at top and bottom to a depth of at least 50mm and set back at least 50mm from the surface of the wall
  - Tie bars to be cut, splayed and grouted into brickwork to a depth of at least 50mm and set back at least 50mm from the surface of the wall

- The bars to be welded to a frame of angle iron with a minimum dimension of 35mm x 35mm x 3mm which is fixed to the brickwork surrounding the window (not to the window frame) by either 75mm x 9mm proprietary anchor bolt for fixing into masonry (e.g. Rawlbolts) or 75mm 5.5mm diameter countersunk woodscrews with suitable proprietary wall plugs at 300mm intervals all-round the opening. Bolts or screws to be spot welded to the frame.
- Alternatively, consider internal or external lockable steel bar/mesh gates, roller shutters, or internal collapsible (folding) steel grilles. These should be professionally fitted and ideally be certified as meeting a recognised security standard (see the list at the end of this guidance).

Locks

There are a wide range of security locks available to purchase. These include 5 lever mortice deadlocks, 5 (+) pin cylinder/Euro locks, multilocks, padlocks and magnetic locks. The complexity and quality of lock design and manufacture is fundamental to the level of protection provided. A summary of related British / European standards is included at the end of this guidance.

Locks often come within the door set itself or are fitted after the door itself is positioned. In all cases, ensure that an approved mortice lock is fitted, where a bolt throws from the door into the frame itself. Where non-standard locks are used, a second lock can be installed to add to the security of the door. Where access control locks are installed (e.g. fob controlled maglocks) these should not be relied upon as the sole means of securing the site out of hours – there should be a deadlock fitted as well.

Note that the use of BSI certified locks may be an insurance requirement.

Intruder Alarms

Intruder alarms are often an insurance requirement. They provide a high level of theft deterrence as well as early notification of unauthorised entry.

Intruder alarm systems should only be installed and maintained by a company that is certified to do so by the NSI or SSAIB in the UK. This will mean that they will be recognised as a compliant company by the relevant responding police force and will install and maintain in accordance with the appropriate standards.

Unless more specifically confirmed, the security grading of the intruder alarm system (detection and control equipment) for many commercial premises should be to Grade 3 as detailed in EN 50131 and PD 6662 (UK only). It should also be a “confirmable alarm” as detailed in BS 8243 (UK), which means that after an initial detection, a second sequential detection (another detector) can then confirm the initial alarm detection to the alarm receiving centre (ARC) in order to reduce false alarms.

It is also likely that remote signalling to an ARC will be a condition of insurance cover. The ARC should be one that is inspected and certified by a nationally recognised security body and compliant with police requirements. In some circumstances, where guards are on site 24/7, alarms may be monitored in house.

Alarm signalling will need to be by a Dual Path (DP) remote signalling product that has been tested and certified to BS EN 50136 or PD 6669 (UK only). For many commercial premises, insurers will require such DP signalling to meet the specification for DP3 or DP4, as set out in those same standards.

A formal Police response may also be required. In the UK, in order to be eligible for a Police response, a police Unique Reference Number (URN) will be required. In order to obtain this, the alarm system needs to transmit “confirmable” alerts to the ARC as detailed earlier. To obtain a URN, and be eligible for a Level 1 Police response, the alarm system will need to:

- Comply with the standards detailed earlier
- Be maintained by a nationally certified company
- Be monitored by a Police approved ARC

Certified alarm companies and your insurance contact will be able to advise on all of these requirements.

If the alarm is activated (whether the activation is confirmed or not), or any signalling path is lost, the appointed keyholders will need to attend the premises (preferably not alone, and in a safe manner) immediately to investigate the reason for the activation.

Response to an alert, fault or call from the ARC must be by site staff who can attend within 20 minutes or a professional (e.g. in the UK, Security Industry Association (SIA) approved) keyholding company, even if the police have responded.

If there is a fault with the alarm system or an alarm signalling path, an alarm technician should be called and the keyholders should not leave the premises unattended until they are fully re-secured, with the alarm system and its signalling paths fully reset.

Inform Insurance representatives immediately if there is a notification of a reduced level or withdrawal of Police response to the intruder alarm system; this withdrawal may happen after 2-3 false alarms in any given 12 month period.

Never leave the premises unattended, unless physically secured and the alarm system is fully set including the designated methods of remote signalling.

Telephone networks around the world are being upgraded in such a way that alarm systems will need to communicate to the ARC using Internet Protocol (IP) technology rather than traditional copper based phone lines. The same applies to mobile phone technology, as the 3G network will no longer be able to carry alarm signals. Check with your alarm companies

and communications providers in all cases to ensure that your alarm system will operate with these changes in place.

The following provides further good practice guidance suitable for most commercial and industrial premises:

- Except for ancillary control equipment (such as remote keypads and digital key readers), control and signalling equipment should be located in a position where it is concealed from general view and is least vulnerable to attack
- Ensure that there are no items of value on the alarm's entry/exit route (i.e. near the entry door or alarm keypad), so that such items are within alarm confirmation zones not on the entry/exit route
- Audible warning should be by either two external self-actuating audible warning devices or by one external self-actuating warning device and an internal self-actuating siren or two tone electronic sounder, each giving a sound emission of at least 100dB at 1 metre
- Where it is not possible to install an external warning device above 3 metres (i.e. so that it would not be readily reached from ground level), fit two external self-actuating warning devices. They should be sited on different elevations of the premises, where possible
- Where the system has remote signalling, which is usually desirable, site any internal warning device remotely from the control panel so as not to identify the position of the panel when activated. For the same reason, any internal sounders used as part of the alarm setting / unsetting procedure should also be sited remotely from the control panel
- The means of unsetting should be via an entry door lock linked to the alarm or the use of a remote-control device (transmitter or fob) upon entry
- Some alarm companies will wish to maintain intruder alarms remotely, without visiting the premises. Note however, that maintenance visits should be on site and at least every 6 months.

Guarding

Traditional security guarding remains a mainstay in security strategy. To help ensure that security guards provide a good quality defence they should be subject to suitable background checks and certifications, and suitable onsite systems such as guard tour verification.

In the UK licensed security personnel can be contracted from firms that are approved by the NSI, SSAIB or the SIA Approved Contractor Scheme.

Guarding solutions should be carefully managed and should integrate with all other security measures. Where guards are in use, it is advisable to have 2 guards deployed rather than sole guards, each with suitable means of communication to allow them to request assistance at any time.

Protection of Unoccupied Buildings

Fire, theft and malicious damage in empty premises is a significant cause of loss. There is evidence to suggest that once a building has been vandalised, further attacks can occur within a short period of time.

Good management procedures including regular inspection visits (at least once a week) and regular maintenance of the property and its fire and security systems can help to prevent criminal attacks and also reduce the eventual cost of remedial work should a loss occur.

It is important to ensure that the fabric of the building is maintained and kept in good order. Without regular maintenance an unoccupied property can quickly become run-down and attract unwelcome attention, such as from vandals and fly-tippers. Graffiti should be removed and any damage repaired without delay.

Unoccupied buildings are an attractive playground to children. Children and other trespassers are owed a duty of care such that even unoccupied buildings need to be maintained as safe environments as far as reasonably practicable. Unoccupied buildings should of course be maintained as safe environments for those with legitimate access.

Best practice precautions should include the removal of all non-essential contents and services. However adequate physical security and alarms should be maintained. Further mitigation can include the use of guarding, boarding of windows/doors and the use of temporary alarms.

Security Fogging Devices

A Security Fogging Device is an electronically operated security system, which on activation produces a dense “fog” in order to disorientate a potential thief and deter/hinder further access into the protected area.

Fog is produced by passing glycol (or other fluid) through a heating block, where it vaporises before being emitted into the area to be protected. As the vapour is released into the atmosphere it instantly condenses to form a dense white fog. Glycol based products are considered to be non-toxic.

Security fog may be combined with flashing lights and sirens to further disorientate potential thieves. These systems are typically used in retail environments and careful consideration should be given to employee and customer safety.

Security Fog Devices should be designed, installed and maintained in accordance with the manufacturers specifications and conform to BS EN 50131-8 in conjunction with insurers requirements.

Document Number: RCG401 v3 Date: 01/2025

Cash Security and Defence against Robbery

Cash continues to be one of the most thief attractive commodities. Businesses most at risk include those dealing with high value easily transportable goods such as jewellery, designer clothing, portable electronic devices, tobacco products, wines and spirits. Cash related operations such as post offices, pawnbrokers, book makers and petrol filling stations are also at high risk of being targeted. Cash dispensing machines also increase the likelihood of an attack as do late night working hours.

Where possible, the amount of cash held at any given time should be minimised. Cash holdings can be further reduced by making/receiving payments by cheque or electronic transfer.

Staff involved with cash exposures, even those not directly handling cash can find themselves involved in a threatening situation simply through their presence at the scene of a criminal attack.

As well as having a good layered defence at the premises, there are a number of further measures that can be deployed to mitigate the risk, which include:

- Securing cash and valuables in approved safes (typically safes have Eurogrades that determine acceptable cash limits
- Sound management and procedures when handling cash – e.g. secure the room before opening the safe, ensure 2 people present while the safe is open and limit the time the safe is ever open
- Reinforcement of cash rooms, doors and glazing
- Use of professional cash carriers
- Removal of cash from site by couriers on a frequent basis
- Use security devices such as safe alarms and time locks
- Ensure that safe keyholders are separate to those with keys that access the building itself
- Security fogging devices

The standards and resources listed at the end of this guidance provide more detailed information.

Computer and Electronic Equipment Security

Computer and other electronic office equipment in business premises are particularly attractive to thieves. The impact of theft is not just related to the loss of hardware but may also compromise data security and cause significant business interruption.

In environments where thieves may operate, which includes open plan office environments, portable computer equipment should be locked safely away or secured to the workstation when not attended. Care should be taken that securing equipment is compatible with the computer equipment and associated warranties.

In environments where higher value items are used/stored (server rooms for example), there are a number of devices and solutions such as secure areas, cages, anchoring equipment etc. that can be deployed to minimise the risk of theft. Additionally, there are many procedural measures that can be employed to reduce risks.

See the standards and resources at the end of this guidance for more details.

Fuel Crime

Above ground diesel tanks at farms, goods storage locations and domestic premises are a target for fuel thieves.

Collateral damage following fuel theft can often lead to fuel leaks contaminating the ground with associated high clean-up costs.

Given this theft risk, all fuel storage facilities should be subject to a suitable risk assessment.

Fuel tank theft security measures include:

- Isolation of electric pumps
- Closed shackle padlocks on filler caps
- Anti-siphon devices
- Minimising fuel levels
- Appropriate access controls, fencing, lighting, CCTV and alarms where practical

Metal Theft

The rising worldwide demand for metals has resulted in a significant increase in their market value which in turn has led to a very serious rise in the number of metal related thefts, particularly of non-ferrous metals such as copper and lead.

Many of the losses have involved thieves targeting unoccupied buildings for copper cabling, pipework, sanitary fittings and lead from roofs.

In addition to the cost of replacing stolen property, the damage caused to the fabric of the building through its forced removal can also incur very large repair bills. Where the theft of lead from roofs has not been detected quickly enough, losses have been greatly increased due to subsequent damage caused following rainwater ingress.

It is important to identify all of the potential at risk areas – stock, building fittings, lead roof tiles, plumbing/pipes, cabling/cable trays, boilers, plant room equipment, fences/gates/posts etc. as some may not be obvious.

Solutions include those already detailed within this guide (secure areas, alarms, CCTV etc.). The use of security tagging/marking schemes can also be a benefit.

Standards and Further Resources

The following list details resources, guidance and formal standards in use in the UK. References to some European sources and standards are however also included.

Key resources

RISCAuthority (the UK property insurers' technical advice body) is an authoritative source for information on all of the subjects and security measures in this guidance. RISCAuthority is a free resource and is available at Index of Resources | Fire Protection Association.

There are a large number of British and European Standards with the prefix of (BS, EN, PAS and PD) relating to the security topics covered in this guidance document that can all be found at **British Standards Institution** www.bsi-global.com. Many of the relevant ones are listed below.

The **Loss Prevention Certification Board (LPCB)** scheme (run by the Building Research Establishment (BRE)) has many Loss Prevention Standards (LPS) that provide guidance on various security measures, as well as security products that have been tested to meet strict security criteria and grades. These can be found at www.redbooklive.com.

Secured By Design (SBD) is an official police security initiative that aims to "improve the security of buildings and their immediate surroundings to provide safe places to live, work, shop and visit". There is a lot of good security advice and guidance here at www.securedbydesign.com.

European Committee for Standardisation (ECN). There are three European Standards Organizations (ESOs): CEN, CENELEC, and ETSI. The mission of the European Committee for Standardization (CEN) provides a platform for the development of European Standards and other technical specifications. CEN is a major provider of European Standards and technical specifications, similar to the BSI in the UK, and is the only recognized European organization for the planning, drafting and adoption of European Standards in all areas of economic activity. The only exceptions are:

- Electrotechnology (European Committee for Electro-technical Standardization - CENELEC)
- Telecommunications (European Telecommunications Standards Institute - ETSI)

ECN can be accessed here - https://www.cen.eu/

Standards and further guidance

General security guidance (further to those above):

- The British Insurance Brokers Association (BIBA) – www.biba.org.uk/
- Association of British Insurers - www.abi.org.uk
- Confederation of Fire Protection Associations (Europe). While much of the resources listed will be relevant outside of the UK (many of the standards apply in both the UK and EU), the following website is a useful source for some generic security measures across Europe:
  http://cfpa-e.eu/cfpa-e-guidelines/guidelines-security-form/

Regulatory and trade bodies:

- Security Industry Authority (SIA) - www.gov.uk/government/organisations/security-industry-authority
- The National Security Inspectorate (NSI) – www.nsi.org.uk
- British Security Industry Association (BSIA). www.bsia.co.uk/
- The Security Systems and Alarms Inspection Board (SSAIB) – www.ssaib.org

Security fences/Ram raid:

- BS1722:10:2019 Specification for chain-link and welded mesh anti-intruder fences. This type of fence can be considered suitable as a general purpose or low security fence. Where enhanced levels of security are required BS1722 part 12 or 14 should be specified
- BS1722:12:2019 Specification for Steel Palisade anti-intruder fences. This type of fence can be considered suitable for all types of fencing from general purpose to extra high security fencing
- BS1722:14:2019 Specification for open mesh steel panel fences. This standard specifies the requirements for four standards of open mesh steel panel fence ranging from fences suitable for boundary and general purpose to fences suitable for extra high security
- BS1722:17:2019 Specification for electric security fencing - design, installation and maintenance. This standard specifies the requirements for electric security fencing
- PAS 68 and PAS 69 relate to ram raid defences and vehicle barriers

CCTV:

- BS EN 62676-1-1:2014 - Video surveillance systems for use in security applications. System requirements. General
- BS 8418:2015+A1:2017 - Installation and remote monitoring of detector-activated CCTV systems
- NPCC Police Requirements & Response to Security Systems Policy or Police Scotland policy
- The Information Commissioner's Office (ICO) – Code of Conduct for CCTV
  https://ico.org.uk/

Buildings, doors, hatches, shutters and glazing:

- BS 8220-2:1995 - Guide for security of buildings against crime. Offices and shops
- BS 8220-3:2004 - Guide for security of buildings against crime. Storage, industrial and distribution premises
- LPS 1175:2019 Requirements and testing procedures for the LPCB approval and listing of intruder resistant building components, strongpoints, security enclosures and free-standing barriers
- BS EN 1627:2011 Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification
- BS 5357:2007 - Code of practice for installation and application of security glazing (high resistance to attack)
- **PAS 24:2016 – criteria for testing windows and door sets against casual burglars. This PAS applies** to manual attack testing of single leaf domestic doorsets and windows, including locks (but excluding picking/sawing) and hinges
- **BS EN 356:2000 – code of practice for security glazing and resistance to manual attacks**
- BS EN 1063:2000 - the standard for bullet resistant glass
- BS EN 1522:1999 and BS EN 1523 - standard required for frames for bullet resistant windows, shutters and blinds
- *LPS 1270*: Issue 1.1. Requirements and testing procedures for the LPCB approval and listing of intruder resistant security glazing units
- Door and Hardware Federation (DHF) - http://www.dhfonline.org.uk/
- Glass & Glazing Federation – www.ggf.org.uk

Locks

- BS EN 12209:2016 – specifications for door locks, relating to other standards below. This is a UK version of a European Standard for door locks. Numerous different combinations (Grades) of lock case/lock mechanism and key security are available, plus related testing for attack resistance, force, durability, fire and safety
- BS x621 series. The one most common standard is BS 3621, evolving into the x621 Series, which sits alongside European Standards for door locks (EN 12209 (above) and EN 1303 (below))
- BS 3621: 2017 – 5 lever mortice deadlocks, cylinder deadlocks and rim locks that can be opened from either side by a key
- BS 8621 – as BS 3621 but with no key required to exit (e.g. thumb lock)
- PAS 3621 - For multi-point locks with keys required both sides
- PAS 8621 - For multi-point locks with keyless egress
- BS EN 1303:2012 Cylinder lock specifications (will still require to meet TS007/SS312 below). This is a UK version of a European Standard for lock cylinders. Various security levels against attack and for key security are available

- TS007 (3 star level) and SS312 – cylinder lock resistance to snapping attacks. This is a UK Standard developed to recognise and protect against the risk of 'snapping attacks' on door lock cylinders. Snapping attacks relate to a form of criminal attack whereby a protruding cylinder is gripped by a wrench, or similar tool, and twisted until it snaps in its narrow middle section. TS 007 cylinders with a 3 Star rating can resist such attacks on their own, but a 1 Star cylinder needs to be married up with a 2 Star surrounding door handle to give an overall 3 Star level of protection
- BSEN 12320:2012. This standard reflects a European Standard for padlocks and staples (padbars) of all types, i.e. open and closed shackle. Security Grades range from 1-6, 6 being the highest.
- BS EN 179:2008 & BS EN 1125:2008 - for emergency escape door mechanisms. These standards are UK versions of European Standards for emergency escape door mechanisms at premises where, respectively, no panic is likely to occur, e.g. a factory/office, and those where it might, e.g. a shop or club/pub. Where an external keylock is incorporated, it should be tested to a security level chosen from BS EN 12209 (for external attack only)
- Master Locksmiths Association (Sold Secure scheme) www.soldsecure.com

Intruder alarms

- PD 6662 and BS EN 50131 – relates to the various types and installation of intruder and hold up alarms
- LPS 1277, PD 6669 and BS EN 50136-1 refer to alarm transmission systems
- BS 8243:2021 – relates to 'confirmable' alarm requirements
- BS 9263:2016 refers to remote technical access into alarm systems
- BS EN 50518:2019 – best practice for ARCs
- SSAIB Code of practice for temporary alarms
- NPCC Systems Security Policy https://www.policesecuritysystems.com/

Keyholding services, guarding, couriers

- BS 7984-1:2016Keyholding and response services. General recommendations for keyholding and response services
- BS 7499:2020 – Static Site Guarding and Mobile Patrol Services, Code of Practice

Security fogging

- BS EN 50131-8:2009. Alarm Systems Intrusion and hold up systems – part 8

Safes, strong rooms and ATMs

- BS EN 1143-1:2019 - Secure storage units. Requirements, classification and methods of test for resistance to burglary. Part 1 - Safes, ATM safes, strongrooms. Part 2 where deposit systems are incorporated

- The LPCB scheme (LPS 1175:2019) also provides details of approved safes and strong rooms all of which comply with this standard above
- LPS 1183 Part 1: Issue 4.3 Requirements and testing procedures for the LPCB approval and listing of safe storage units Part one: Safes and strongrooms
- BS 7582:2005 British Standard Code of Practice for Reconditioning of Used Safes
- BS 7872:2011 - Code of Practice for Operation of Cash In Transit Services
- European Certification Board - Security (ECB-S) scheme

Computer physical security

- Loss Prevention Standard (LPS) 1214 (#2) - **anchoring and enclosures**

Others

- Your local Crime Prevention Officer
- Cyber security for business - https://www.ncsc.gov.uk/ - click on “Information for…”

For further advice please speak with your normal insurance advisor

Document Number: RCG401 v3 Date: 01/2025