RISCAuthority

administered by

FPA Fire Protection Association

S34 Intruder alarm systems: Ten-step guide for purchasers

Version 2 Published 2022

Cover image: Getty/Ceri Breeze

IMPORTANT NOTICE

This document has been developed through RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various RISCAuthority Working Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

FPA has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, FPA makes no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, FPA makes no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state-of-the-art technologies current at the date of this document.

Use of, or reliance upon, this document, or any part of its content, is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude), entirely or in part, mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it, or any use of, or reliance placed on, the content of this document or any part of it.

Contents

1 Introduction

Intruder alarm systems are a means of protecting both commercial and domestic premises against theft, robbery, malicious damage and arson. Premise owners or occupiers may find that their insurers make certain types of insurance cover conditional upon having such a system. Insurers will usually require an alarm system to meet certain requirements, as outlined in this guide.

It should be noted that effective alarm systems can be a complex and significant investment. Time spent researching options should help inform discussions with prospective alarm installers, and thus help to choose the most appropriate alarm system.

This ten-step guide outlines insurers' likely main requirements/ recommendations for an intruder alarm system. Following them will help ensure that any new alarm system is both acceptable to insurers and is a reliable and sound investment.

A summary of the guidance is included as Appendix 1 and Appendix 2 for police response intruder alarms and audible-only alarm systems.

> **Note:** If you require further information on the design and use of these, or other types of, alarm systems, there are several RISCAuthority guides on intruder alarm systems and related matters, which are available as free downloads from the RISCAuthority website www.riscauthority.co.uk

2 Basic elements of an alarm system

Alarm systems consist of three basic elements:

- Detection devices
- Control equipment
- Signalling equipment.

The detection devices (typically including door contacts, movement or vibration detectors and sometimes 'hold-up' buttons), together with alarm signalling equipment are connected to the control equipment (the 'panel') – which acts as the 'nerve centre' of the system.

Although performing a distinct, separate function, the signalling equipment is often incorporated into the panel. The purpose of the signalling equipment is to transmit a signal if the alarm activates. It can do this 'locally', e.g. by operating sounders on the outside and/ or inside of the building, or 'remotely', e.g. by sending signals to a police recognised Alarm Receiving Centre (ARC). Most police response alarm systems have both local and remote signalling.

> **Note:** Individual insurers will have their own specific criteria on minimum standards for signalling paths. Refer to insurer for guidance.

3 Ten step guide to buying an intruder alarm system

3.1 Step 1 – Selecting an installer

3.1.1 Police response intruder alarm system

To qualify for a routine emergency police response to an intruder alarm, use an installer and alarm receiving centre (ARC) that are regulated by one of the police recognised alarm inspectorates, namely the National Security Inspectorate (NSI) or the Security Systems and Alarms Inspection Board (SSAIB). The ARC will usually be selected by the installer.

NSI/SSAIB supervision of installers helps ensure that alarm systems are designed, installed and maintained by suitably trained, competent and trustworthy personnel in accordance with relevant British/European standards.

For further information and details of approved installers in your area, please visit nsi.org.ukand/orssaib.org.

3.1.2 Audible-only alarm systems

Audible-only is a term used to refer to alarm systems that rely entirely upon alarm sounders installed at a premises to raise a local response – typically from people who may be living or working at, above or in the immediate vicinity of them.

Note: A 'speech dialler' device (which can telephone a series of pre-programmed phone numbers and play a recorded message and/or send a text) has been a useful option to enhance audible-only alarm systems. However, diallers are not permitted to contact the police or Alarm Receiving Centres (ARC),and as such do not qualify as 'remote signalling' (or as a 'remotely monitored' alarm) for insurance or police purposes. Also, BT will discontinue PSTN (Public Switched Telephone Network) and ISDN (Integrated Services Digital Network) and BT phone lines will be replaced with VoIP (Voice over Internet Protocol) systems by 2025. Speech diallers using PSTN and ISDN technology will become redundant.

3.2 Step 2 – Consulting your insurer

Where insurers credit intruder alarm system for property theft protection, they will normally stipulates requirements, or otherwise provide general guidance.

It is recommended that your insurer or your normal insurance adviser is contacted for advice on suitable alarm systems, and this advice be passed onto installers, rather than expect the installer to contact them directly.

Important note: An insurance policy may contain a condition that requires:

- a particular type of alarm installer, system, signalling and response;
- an emergency/routine maintenance contract being kept in force;
- provision to the installer and others of key holders' details;
- the insurer's prior approval for any changes to the system;
- the insurer to be notified if police response is reduced or withdrawn;
- full setting of the alarm system, including all means of communication with the ARC, whenever the premises are left unattended (and possibly partial setting at other times);
- keeping any alarm operating codes secret and not leaving alarm operating devices at the premises when they are unattended; and
- prompt key holder attendance after any reported alarm activation or fault.

Policy conditions vary between insurers, so you should check your own policy for details of any such condition, and whether failure to comply could jeopardise insurance cover.

An advantage of obtaining prior insurer guidance is that prospective installers will be competing against a common specification.

3.3 Step 3 – Security grades

When designing an alarm system, installers regulated by the NSI or SSAIB are required to conduct a formal security risk assessment. This is to help determine a security 'Grade' for the system (detection and control equipment) and signalling, plus other system design features, most appropriate to each customer's circumstances. Insurers treat grade of system and grade of signalling as separate issues and their likely stance on each can be summarised as:

- System (detection and control equipment)

Grade 1 – Inadequate for insurers' needs. Intruders expected to have little knowledge and limited tools. Alarm is suitable for a low risk.

Grade 2 – Suitable for most domestic and some low risk commercial premises. Intruders expected to have limited knowledge and some tools. Alarm is suitable for a low to medium risk.

Grade 3 – Suitable for most commercial, and some high risk, domestic premises. Intruders expected to have knowledge and full range of tools. Alarm is suitable for medium to high risk: a (Grade 3 option E4) dual path remote signalling will usually be required, plus an external alarm sounder.

Grade 4 – Suitable for very high risk premises. Intruders expected to have sophisticated knowledge and tools. Alarm is suitable for a high risk.

Important note: Selecting the correct grade of system and signalling at the outset is very important, as the grade of equipment cannot usually be later changed to another grade without buying and replacement components.

When it comes to grades of system (detection and control equipment) the common choice at most premises is likely to be between Grades 2 and 3. The main differences between them are that Grade 3 systems can record more information in their memory (event log), have better mains power monitoring and battery back-up, and have movement detectors that:

- prevent or detect re-orientation (changed field of view); and
- detect 'masking' (blocking or covering the detector).

At many commercial, and a few domestic premises, the nature and value of the property at risk will be such that a Grade 3 system will clearly be most appropriate.

In cases of doubt, a factor that may suggest the need for a Grade 3 system is the risk of interference with alarm equipment when the alarm is unset (particularly movement detectors), either by members of the public or by staff. This can be a particular risk with, for example, premises such as shops, pubs, clubs, car showrooms or leisure facilities etc, where the public may have unsupervised access during business hours, or for those businesses that have a large or transient workforce where trustworthiness is difficult to monitor.

Figure 1: Movement sensors can be vulnerable to interference

When it comes to grades of signalling, installers may simply suggest a grade of signalling that matches that of the system. However, there are significant differences between the remote signalling notification options and corresponding fault reporting times within the overall system grades; principally in how quickly any failure, for example, cutting of the telephone line, will be detected and notified to the ARC. Given the importance of remote signalling to the overall effectiveness of the system, Grade 3 Option E providing a maximum time-interval of 3 minutes for loss of one signal path will very often be the most appropriate choice, whatever the underlying grade of the system.

Important note: In cases of doubt as to which system and signalling grade is appropriate, the safe theft-insurance default is to select Grade 3 control equipment and Grade 3 option E dual path signalling.

3.4 Step 4 – Risk assessment process

Installers cannot be expected to anticipate every aspect of an individual customer's risk exposure, so purchasers should fully co-operate in the risk assessment process. If you are not asked about certain issues that seem relevant to you, ask the installer to take them into account, or explain to you why they do not think they are relevant. Some matters that may be overlooked include:

- **Insurer requirements:** has your insurer made any requirements or offered advice?
- **Risk of sabotage of equipment or signalling:** for example,has the installer fully accounted for the risk that movement detectors could be covered, or that phone lines used for signalling could be cut?
- **Business interruption:** monetary values of target items are not the only indictor of the need for a higher grade system. Has the installer considered the risk of lost trading or damage to business reputation, following theft of important items or records,or damage to the premises or vital production machinery, following arson or malicious damage?
- **Future risk:** the costs for Grade 3 versus Grade 2 equipment, is often marginal, so it may be worth buying a higher grade system now, as this could avoid later upgrade costs if target risks increase.
- **Police response and key holder safety:** the aim should always be to obtain a police response early on in any break-in; not only to reduce the size of any loss or increase the chance of an arrest, but also to provide timely assistance and reassurance to key holders. Where employees are key holders, health and safety responsibilities are an important consideration. As such, the risks of attending alone ('lone working') should always be considered in determining alarm system design.

3.5 Step 5 – Sequential confirmation (system design)

To minimise the risk of police being called out to false alarms, new police response alarm systems must be of a type capable of generating what are called 'confirmed activations'. Sequential confirmation is the format most used and requires that the ARC receive two or more alarm-related conditions, within a certain time period, before they can ask the police to attend.

Whilst the police will only respond to confirmed activations, key holders are expected to respond to both confirmed and unconfirmed activations. To help ensure that key holders are not called out without suitable police response, it is important that the design of a confirmation alarm system ensures that:

- there are sufficient detection devices to ensure that a confirmed activation is obtained early on during any break-in;
- any detrimental security impact that might result from the designated 'entry/exit' door, where the alarm is set, being forced open by intruders is minimised; and
- suitable dual path signalling is provided.

These issues are each expanded upon below.

> **Note:** Sequential alarm detection for confirmable alarm systems is (since 2021) optional per BS 8243 and can instead be Video Surveillance Systems (VSS) or audio confirmation. This needs to be set up in accordance with various standards: advice can be sought from ARCs.

3.5.1 Detection and control equipment

Insurers will be looking to see that systems have been designed to generate a confirmed activation from all ‘at risk areas’ (areas containing ‘target items’, that is items which are expected to be of attraction to criminals) as soon as possible after an intruder enters them. This typically involves having at least two different forms of detection device at, or near, each possible entry point.

In addition, the alarm system control and signalling equipment should be located in an area concealed from external view, and itself alarm protected in such a way that intruders cannot reach it without creating a full alarm activation.

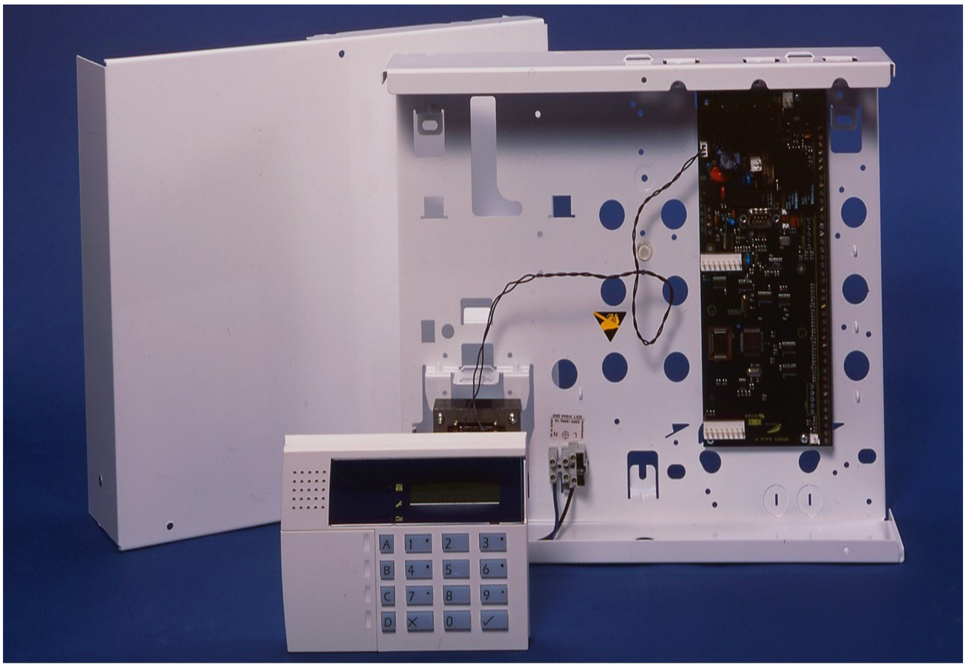

Figure 2: The control and remote signalling equipment should be installed out of sight and in a secure area Figure 2: The control and remote signalling equipment should be installed out of sight and in a secure area

3.5.2 Unsetting

Alarm users need to have a method of switching off an alarm system without causing a false alarm. There are a variety of ways that this can be done, but it is likely that the installer will propose one of two methods:

- Using a door lock linked to the alarm: when alarm users unlock a designated entry door (fitted with a lock electronically linked to the alarm), the alarm system turns off its confirmation capabilities. Thereafter, the user can enter the premises and fully unset the system by entering a security code at a keypad.

> **Note:** An intruder forcing open the entry door will immediately start the process of generating a confirmed alarm. Insurers generally prefer this means of unsetting.

- Using a digital key to unset the system: the system is unset by operating a hand-held transmitter (similar to a car remote control key) or by presenting a proximity card or token (‘fob’) to an electronic ‘reader’. There is a designated entry door through which the user must enter, and an entry timer device. During the entry time alarm sensors covering the entry route will be activated by users, but any resultant alarm activation is held on site to allow the user time to unset the system. If the system is not correctly unset at expiry of the entry time, an unconfirmed alarm will be transmitted to the ARC. After expiry of the entry time, and a further false alarm abort time, a confirmed alarm can be generated – but only after further detectors not covering the designated entry/exit route have activated. With this form of alarm system unsetting, is layout dependent.

> **Note:** An intruder forcing open the alarm entry door will be treated by the system as a potential user, and any confirmed alarm may be either delayed or not obtained at all. Whilst insurers will generally accept this method, they may not do so at premises where significant values of ‘target items’ are within easy reach of the entry door.

Figure 3: A typical portable transmitter

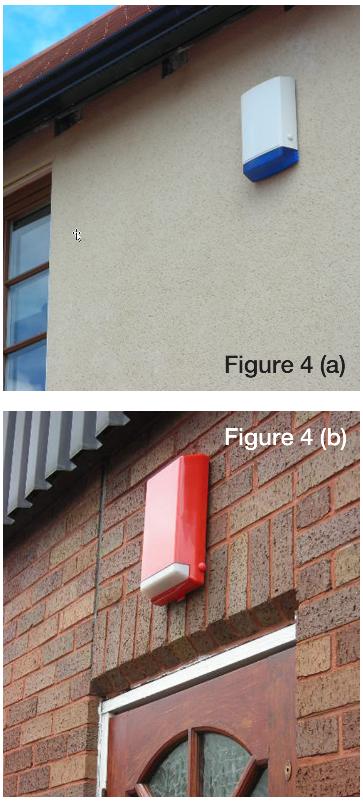

Figure 4: External sounders should be installed at high level, eg 4m above ground, as shown in (a), not (b)

3.5.3 Signalling

To help ensure that alarm events can still be sent to the ARC after a phoneline has been cut, signalling products used in conjunction with sequential confirmation systems need two connections (paths) to the ARC, each using a different type of signalling technology, for example, telephone and radio. Such systems are termed 'dual path' signalling systems.

A critical feature of dual path signalling systems is how soon, if at all, the ARC will become aware of failure of either or both paths, as this may indicate criminal activity and permit them to promptly call the police and key holders.

With remote signalling potentially the weakest link in any alarm system, insurers will usually require a Grade 3 option E or a Grade 4 dual path signalling system to be used, whatever the underlying grade (2 or 3) of the control equipment.

Note that alarm signal grading changed in June 2019, with both old and new grades being referred to by installers and insurers. It is often best to stipulate the dual path (DP) specification rather than the signalling grade – most insurers would expect a commercial premises to have either DP3 or DP4 alarm signalling in place. These will alert the ARC of a failure of both signal paths (catastrophic failure) in either 4 minutes (DP3) or 3 minutes (DP4), which is enough to trigger a Police response where one is in place.

In addition to the remote signalling, insurers will still usually want an external alarm sounder installed for its local deterrent and warning effect. Such sounders can also help police locate the premises to which they are being called. Sounders should be installed at a height and location, where they cannot easily be reached by intruders.

3.6 Step 6 – Hold-up (personal attack) alarms

Hold-up alarms, commonly referred to as personal attack (PA) alarms, are used to alert police to the need for an emergency response to a violent or threatening event.

PA facilities can be an important feature of alarm systems but, because of the risk of (often well-intentioned) misuse, and the consequent impact on police resources, they should only be provided if there is a real risk of an attack. Dual action push button devices are usual and should be located adjacent to the expected area of an attack (to permit their use by someone viewing, but not directly involved in, the attack).

3.7 Step 7 – Alarm response

Insurers value police attendance to alarms as only they have the authority, back-up resources and speed of response to effectively deal with criminal events, and also provide related safety and support for key holders. To obtain police response, arrangements for an immediate 'level 1' response, or the next best available level, need to be put in place by applying for a police Unique Reference Number (URN). Alarm systems installers will arrange this. URNs are issued (and, in the event of undue false alarms, withdrawn) in accordance with the responding police force's Security System Policy (SSP).Details of available response levels and the SSP can be obtained from alarm installers and local police force headquarters.

In addition to the expected police response, key holders (either non-commercial or commercial) need to be appointed for alarm systems, to respond to all (confirmed and unconfirmed) alarm activations and faults, allow others access (the police, for example), and then take any necessary remedial action, including checking that the alarm system can be fully reset, before leaving the premises.

Note: In order to get a Police response for hold-up alarms, these must be configured in accordance with appropriate standards and require a separate police URN.

3.7.1 Non-commercial key holders

Non-commercial key holders will typically be the alarm owner or persons associated with them, for example, for commercial premises members of staff, or domestic premises trusted friends or neighbours. Key holders should reside within a reasonable travel time of the alarmed premises (a maximum of 20 minutes for alarm systems with a URN) and be fully trained in the operation of the alarm system and associated security procedures.

With personal safety in mind, all non-commercial key holders should be advised to:

- carry a mobile phone;
- attend with someone else (another key holder, colleague or companion, etc),
- take care upon arrival at the premises to survey the immediate scene; and
- call for police assistance via the 999 telephone system if there are clear signs of a break-in, and/or if intruders can be seen within.

Where it is not practical or possible to appoint non-commercial key holders, or have concerns about their reliably or safety, a complementary or alternative response, is recommended using a commercial response company.

3.7.2 Commercial key holders

For a fee, commercial response companies will undertake to act as key holders.

Insurers usually prefer commercial response instead of non-commercial key holders, but generally require that the company holds NSI/SSAIB approval, or otherwise complies with Security Industry Authority (SIA) licensing requirements, holds SIA Approved Contractor Scheme (ACS) status and are within a 20 minutes attendance radius of the customer's site.

Use of key-boxes (or "key-vaults") to facilitate access to keys locally at the premises for commercial responders should be avoided, as regardless of the quality of the box, they may still be accessed by criminals to get into the premises and where alarm fobs are available, even deactivate the alarm system.

Important note: The use of key boxes is a clear security risk and is likely to contravene your insurer's policy alarm condition.

3.8 Step 8 – Alarm receiving centres

Your installer will usually arrange for a suitable ARC to handle alarm signals. Some installers have their own in-house ARC, others appoint an independent one.

ARCs will usually handle alarm activations/faults in accordance with their own standard alarm event handling procedures. These will be detailed in a formal 'response agreement', a copy of which should be made available.

It can reasonably be assumed that an ARC will notify the police and key holders of all alarm activations where it is appropriate to do so. However, it should be checked that the ARC will inform key holders immediately of events where a police response may not be available, in particular:

- receipt of any unconfirmed activations (when the system is set);
- receipt of any alarm or power system faults that could affect the operation of the alarm system (when the system is set); and
- failure of any signalling path (at any time).

Important note: Where ARC procedures do not match those noted above, and the ARC will not agree to change them, reference should be made to your insurance contact.

3.9 Step 9 – Making your choice

At the end of the risk assessment and design process, installers will make their written proposals (see Appendix 3) to customers, who then have to consider if they meet their own and their insurer's needs. This can be a complex decision, when different installers will come up with diverse proposals.

At this stage, price, although an important consideration, should not be the sole determining factor. Instead, attention should be paid to the nature and extent of proposed alarm coverage, the ability of the system to produce the required response early on during any attack and its resilience to deliberate interference. The overriding consideration is, in a break-in or attack, will the alarm system do what is expect?

3.10 Step 10 – Training and use

Alarm systems will not perform well if those who use them do not understand how they work and should be used. Training will help maintain intended level of security and avoid many common causes of false alarms.

False alarms are not only troublesome but can be expensive to resolve, particularly if they lead to the withdrawal of police response – a situation that can also affect insurance cover.

Installers should offer full training in the scope and correct use of the alarm systems, which should be implemented by users.

Appendix 1: Summary of insurers’ typical requirements for a police response alarm system

Insurers’ likely main requirements/recommendations for a new remotely monitored police response intruder alarm system are listed below.

- **Installation/maintenance(all apply):**
  - installation by a National Security Inspectorate (NSI)* or the Security Systems and Alarms Inspection Board (SSAIB)* listed installer, eligible to apply for a police URN with the force in whose are a the alarmed premises are located; and
  - have a contract for emergency and routine maintenance in force.
- **Security grading of system (detection and control equipment) to be:**
  - Grade 3 for most commercial risks, Grade 2 for most domestic risks.
- **Sequential confirmation system to be designed, with (all apply):**
  - control and signaling equipment installed out of sight, and not located in an area used as an alarm entry-exit route;
  - two appropriate forms of detection[1] in each ‘at risk area’[2];
  - means of unsetting to be via an entry door lock linked to the alarm unless the entry route or premises are considered low risk, in which case, use of a remote control device (transmitter or fob) upon entry is acceptable.
- **Hold-up alarm facilities (where required):**
  - dual action attack devices sited adjacent to expected attack area.
- **Signalling to comprise (apply):**
  - a Grade 3 option E, dual path,remote signalling product (ideally one independently certified as meeting this Grade, but in any case as agreed by the insurer);
  - a supplementary external self powered audible warning device (sounder).
- **Monitoring to be by an Alarm Receiving Centre (ARC), with:**
  - NSI/SSAIB approval;
  - the ARC notify the police (where eligible) and key holders of all alarm events/faults, including signalling path failures, immediately upon receipt.
- **Response to be by (all apply):**
  - the police, at the highest response level provided for by the responding force’s Security System Policy (SSP);
  - your key holders (owners/staff/friends, etc or a response company).

Note: If a response company is used, NSI/SSAIB listed companies are preferred. Response companies must not store alarm operating codes or devices at protected premises, e.g. in a key box, without insurer approval.

* For further information and details of listed installers in your area, please visit www.nsi.org.uk or www.ssaib.org.

[1] Typical detection devices are door contacts, movement sensors – such as passive infra-red detectors (PIRs), dual technology devices (‘Dualtechs’) or twin motion detectors (TMD) – and vibration sensors.

[2] Areas containing ‘target items’, that is items which are expected to be of attraction to criminals.

Appendix 2: Summary of insurers' typical requirements for an 'audible only' alarm system

Insurers' likely main requirements/recommendations for a new 'audible-only' intruder alarm system are listed below.

- **Installation/maintenance (all apply):**
  - installation by a National Security Inspectorate (NSI)* or the Security Systems and Alarms Inspection Board (SSAIB)* regulated installer;
  - have a contract for emergency and routine maintenance in force.
- **Security grading of system (detection and control equipment) and signalling to be:**
  - Grade 2X.
- **System to be designed with (all apply):**
  - Control and signalling equipment installed out of sight, and ideally not located in an area used as an alarm entry-exit route;
  - an appropriate form of detection1 in each 'at risk area'[2].
- **Signalling to comprise:**
  - one external, self-powered, audible warning device (sounder), located at least 4m above ground level (or any roof or balcony etc, that is readily accessible from the ground).

Note:

a) Where the 4m provision cannot be met, two sounders are advisable, each located on a different elevation of the premises.

b) If a speech dialler is used, GSM diallers are recommended in place of PSTN diallers, as the latter will use normal phone lines – which could be readily located and cut by criminals prior to a break in. Refer to section 3.1.2 regarding technology changes.

- **Response to be by:**
  - persons living/working in or near to the premises who, when the alarm is usually set, are likely to hear the alarm and be prepared to either respond as, or telephone, a key holder.

* For further information and details of listed installers in your area, please visit www.nsi.org.uk or www.ssaib.org.

[1] Typical detection devices are door contacts, movement sensors – such as passive infra-red detectors (PIRs) or dual technology devices ('Dualtechs') – and vibration sensors.

[2] Areas containing 'target items', that is items which are expected to be of attraction to criminals.

Appendix 3: Alarm system documentation for purchasers

Installers are required to document various aspects of alarm systems, as follows.

Security risk assessments

Although purchasers need to be aware of its outcome, it is not a requirement that an installer shows you their risk assessment. However, most installers will disclose it, and some will ask you to sign it.

Insurers will not normally wish to see the installer's risk assessment if it accords with the suggestions of their own guidelines (or specific requirements following a site visit). However, it may be helpful to provide a copy of the installer's risk assessment if you wish to follow a course of action that is contrary to the insurer's general or specific requirements/recommendations.

Specifications

Installers are required to prepare documents detailing the type and position of equipment used in alarm systems. Traditionally called alarm 'specifications', such documents are more correctly referred to as:

- 'system design proposals' (SDPs) – for proposed systems; and
- 'as fitted documents' (AFDs) – for installed systems.

Where an intruder alarm is required by an insurer as a condition of cover, they may ask to see a copy of the SDP or AFD to ensure that the system meets their needs. A copy layout/ detection plan should be requested from the installer as part of (or to augment) the SDP/AFD, as this will greatly assist insurers in making their decision.

ARC response agreement

You will need to complete a document for the installer/ARC providing details of at least two key holders (and preferably more, to allow for holidays, illness etc).

A further document should also be made available, if full details are not included in the SDP, detailing what steps the ARC will take in response to various types of alarm related events or faults.

RISCAuthority

administered by

FPA Fire Protection Association

Fire Protection Association
London Road
Moreton in Marsh
Gloucestershire GL56 0RH
Tel: +44 (0)1608 812500
Email: info@riscauthority.co.uk
Website: www.riscauthority.co.uk