Recommendations

RC3
Part 2

for loss prevention in electronic equipment installations

Part 2: Security measures

FPA
Fire Protection Association

Protecting people, property, business and the environment

InFiReS

LOSS PREVENTION RECOMMENDATIONS

The aim of the FPA series of Recommendations is to provide loss prevention guidance for industrial and commercial premises and systems. The series continues a long tradition of providing authoritative guidance on loss prevention issues started by the Fire Offices' Committee (FOC) of the British insurance industry more than a hundred years ago and builds upon earlier publications from the Loss Prevention Council and the Association of British Insurers.

Lists of other publications on loss control including other documents in the RC series are available at www.thefpa.co.uk and from the FPA at London Road, Moreton-in-Marsh, Gloucestershire GL56 0RH. Copies of publications can be purchased from the FPA at that address or else by calling 01608 812500 or by e-mailing sales@thefpa.co.uk.

Technical contact:

Adair Lewis

Fire Protection Association, 3rd Floor, Hampton House, 20 Albert Embankment, London SE1 7TJ

E-mail: alewis@thefpa.co.uk

CONTENTS

INTRODUCTION

With the increasing dependence of business on the computer, security protection against loss, damage or interference becomes more important. When the possibility of such action is judged to be high or the consequences of loss are deemed unacceptable, a correctly designed security strategy is necessary. This strategy should be planned in consultation with insurers, the appropriate police authority and other interested bodies.

Organisations responsible for designing, installing and maintaining protection measures should operate an effective quality system and be certificated to BS EN ISO 9001 (ref. 1) and apply relevant security standards.

Staff vigilance and adherence to a security strategy, particularly regarding access control arrangements, are vital for achieving proper protection. In order to ensure this, management should appoint persons to be responsible for the maintenance of the strategy. Responsibilities related to other aspects of the strategy also need to be clearly defined.

Security protection should be considered in conjunction with other protection methods. Statistically, the main cause of fires in information technology (IT) and electronic data processing (EDP) facilities is deliberate fire raising. In view of this, the recommendations given in Part 1 of this series, *Recommendations for loss prevention in electronic equipment installations: Fire prevention* (ref. 2), should also be put into practice.

This document is intended to give guidance as to the manner that security precautions should be practiced, depending on the category of the operation as defined below:

- **Category 1:** Facilities which are central to a major organisation or which provide a real-time service operation, such as in banking and manufacturing operations. Interference with operations in this category is likely to result in major business disruption and significant consequential or asset loss.

- **Category 2:** Facilities which are subsidiary to a central operation. These may be dealing with, for example, marketing functions or revenue earnings. Interference with operations in this category is likely to result in short term business disruption with tolerable asset and consequential loss.

- **Category 3:** Small facilities providing local services or individual location service operation. Interference with an operation in this category should cause only short-term loss and a minimal disruptive effect on business. It should be possible to replace equipment in this category of facility within 24 hours.

- **Category 4:** Facilities for general office administration or minor business processes or which are part of a larger complex. In this category, loss will be localised and asset loss will be minimal; it should be possible to easily replace equipment.

SCOPE

This document describes measures to minimise the possibility of loss, damage or interference involving electronic hardware due to the presence of unauthorised persons.

The guidance given, while intended to significantly reduce the risks for Category 1 facilities, as identified in the *Introduction*, can be selectively applied for lower category facilities depending on the criticality of the installation, the size of asset, and potential direct and consequential losses.

This document does not include precautions to be taken to prevent data theft or corruption resulting from unauthorised information access, remote interception of data or 'hacking'. These aspects are addressed in Part 3 of this series, *Protection of data and software* (ref. 3).

1. Definitions

The definitions given in the *Recommendations for loss prevention in electronic equipment installations: Part 1: Fire prevention* (ref. 2) shall apply, together with the following:

1.1 *Facilities*

The IT and associated installations requiring protection in accordance with this document, including:

- computer/server room(s);

- media storage area(s);

- telecommunications room;

- air-conditioning plant;

- uninterruptible power supply (UPS) room.

1.2 *Layered security plan*

A concept of security protection whereby the area to be protected is surrounded by two or more separately identifiable, monitored or physical boundaries.

1.3 *PIN*

Personal identification number.

1.4 *Security strategy*

A plan detailing security installations and procedures designed for the protection of specific areas.

1.5 *Uninterruptible power supply (UPS)*

An arrangement for supplying electrical power placed between a regular power supply and the system to which it regularly supplies electricity. In the event of a power cut or a surge or fall in power then the UPS acts to provide continuous, unvarying, back-up electrical power.

2. Responsibilities

2.1 Responsibility for all aspects of security should be clearly defined and documented.

2.2 Those given responsibility should ensure that relevant parties are consulted before fire and intruder protection systems are installed or modified. Such parties may include insurers, police, fire brigades and local authorities.

2.3 Senior management should take overall responsibility for security. Individual layers of the security protection may be the responsibility of appropriate sub-managers (eg IT manager, IT security manager).

2.4 Facilities staff at all levels need to understand the contribution expected of them toward the successful operation of the security strategy.

3. Security strategy

3.1 Assessment of the risk

3.1.1 In devising the security strategy, an assessment of the risk should be made, preferably at an early security planning stage. The following points should be considered:

- the importance of the facilities to the business of the organisation or its value as an asset;

- the importance or value of the facilities to outside bodies;

- the target to thieves represented by the hardware – there is strong criminal demand for certain 'high end' equipment and components;

- the likelihood of malicious interference or sabotage to the facilities by any person(s), including employees and ex-employees;

- the level of inherent physical and environmental security enjoyed by the premises housing the facilities;

- the ease of access to the facilities;

- the numbers of persons with physical access to the facilities and the frequency of their visits.

3.1.2 After the above and any other local factors have been taken into account, major and minor threats to the facilities can be identified. For example, the main risk may be identified as being from disgruntled ex-employees.

3.1.3 As part of the assessment, interested parties such as the insurers, police and local authorities should be consulted.

3.1.4 The assessment should establish the security system design criteria.

3.1.5 The security strategy should be re-assessed following any change in circumstances which may affect security, such as employees leaving the organisation, and any weaknesses revealed by security breaches (see Section 9), or by security audits (see Section 10).

3.1.6 Emphasis should always be placed on preventing unwanted events rather than providing protection if and when an event happens. Direct and indirect risks that may lead to such events need to be identified at an early stage so that appropriate action can be taken.

3.2 Location

3.2.1 The building housing the facilities should be located in an area where there is negligible risk from vandalism. A low crime-rate area is preferred.

3.2.2 The facilities should not be directly accessible from outside the building.

3.2.3 Factors identified in Part 1 of this series (ref. 2), should also be taken into account when choosing the location.

3.3 Layered security plan

3.3.1 The design criteria established in the assessment (see 3.1.4) and the location of the facilities (clause 3.2) should be used to provide a basis for a layered security plan.

3.3.2 The layered concept comprises security barriers forming an incremental filter – so that the inner layer, that surrounding the facilities themselves – can only be entered by persons with authorised access.

3.3.3 The plan should be designed to restrict access, as illustrated in Figure 1. The criticality of the facilities and complexity of the surrounding area will dictate the number and type of layers for any given situation. However, it is recommended that buildings housing Category 1 facilities have at least four separate layers.

Layer	Persons permitted access through layer
Layer 1: Perimeter	Persons employed or who have business within the building(s) and areas surrounding the building(s).
Layer 2: Reception/ surrounding areas	Persons authorised to enter 'staff only' areas
Layer 3: Building	Persons authorised to enter the building(s) housing the facilities.
Layer 4: Location of IT facilities	Persons with a legitimate need to gain access to the facilities.

Figure 1: Example of a facility protected by layers of security

3.3.4 Other factors, such as the time of day and local practicalities, would also determine the correct security strategy, and the type and number of layers at any given time.

3.4 *Breaches of security*

3.4.1 Consideration should be given to the possibility of breaches in the security that may result from circumstances foreseen or unforeseen. Such breaches may occur, for example, during a fire alarm when unchecked access to the operation containing the facilities may be possible. The possibility of such breaches should be accounted for in the strategy, such as by the monitoring of emergency exits for higher category facilities.

3.4.2 Methods chosen to limit the possibility or extent of such breaches should not adversely affect emergency procedures (see 4.1.7).

4. **Security control**

4.1 *Access control*

4.1.1 All premises where computers are in use should be subject to a suitable and sufficient risk assessment which will, among other issues, assist in identifying appropriate security measures for the building. Enhanced measures should be considered in all cases where critical information is handled on single personal computers, or where networked personal computers are in use. Additional information regarding assessing the risk of computer facilities is set out in BS 6266 (ref. 4).

4.1.2 In order to restrict access to authorised persons, access control should be adopted at the entry and exit points at all layers of security.

4.1.3 Access control methods can vary from simple recognition of a person or their organisation at a reception desk, through to high-security electronic access control systems (see section 5.3) or mechanical locking systems in conjunction with security personnel. Factors determining the methods used include:

- the level of security required;
- the frequency of access;
- the practicalities of control at particular access points;
- the degree of flexibility required in changing the controls in the event of, for example, employees leaving.

4.1.4 Control methods may be different for each of the layers, but should, in general, be of a progressively higher degree of security from the outer layer inwards. For example:

Layer 1: recognition or identification of persons/ organisation or electronic access control;

Layer 2: as above plus display of identity badge/pass;

Layer 3: as above plus supervision (unless a member of the organisation with high-level clearance);

Layer 4: as above plus high-security access control (including PIN recognition) and/or screening by dedicated, professional security personnel.

Note 1: If electronic access control is employed (see 5.3), access is progressively restricted moving from layer to layer.

Note 2: For certain types of high-sensitivity operation, individual screening in depth must take place at Layer 1, as the chance of an unauthorised person gaining access to the site cannot be tolerated.

4.1.5 Any identified breaches in the access control system should be promptly investigated and result in an appropriate corrective action.

4.1.6 Where practicable, there should be only one entry point to each building containing facilities, although there may be several exit points for emergency purposes.

4.1.7 All entry/exit points should be supervised or secured. Fire exits should be fitted with alarm protection.

4.1.8 Any method of access control should not prevent or hinder evacuation in the event of fire or mains power failure.

4.1.9 Whatever method is deemed appropriate, keys, code numbers and the like should be issued to a minimum number of authorised persons. If electronic controls are used it is recommended that the code numbers are changed periodically. It is also recommended that mechanical lock and key systems are changed whenever an inventory reveals that a key cannot be accounted for. Serious consideration should be given to changing the locks or codes of critical Installations as a matter of routine when an authorised person leaves employment under duress.

4.1.10 Wherever possible, mechanical locking systems should comply with BS 3621 (ref. 5).

4.2 *Perimeter control*

4.2.1 In order to ensure that areas surrounding the buildings are protected against unauthorised access, the perimeter should be secure.

4.2.2 The use of physical barriers, such as fencing (see the appropriate parts of BS 1722, ref. 6), walls or environmental features, may offer adequate protection in some cases but these may need to be enhanced by the use of security personnel (see 6.1) and electronic security such as CCTV (see 5.2), together with adequate security lighting.

4.2.3 If the method of monitoring the perimeter is based on visual means, then a clear line of sight

is essential and should be maintained. This may involve the clearing of trees and the enforcement of parking restrictions.

4.2.4 Perimeter entry and exit points should include access monitoring and control, as appropriate.

4.3 *Building control*

4.3.1 The building(s) housing the facilities should be of sound construction, such as brick or reinforced concrete, offering substantial resistance against physical attack. The building(s) should also have the necessary fire resistance as described in Part 1 of this series.

4.3.2 Ideally, the shell of a key building will be unfenestrated. However, should glazed apertures be featured, critical operational processes should not be visible from outside.

4.3.3 Accessible glazing should be protected against unauthorised entry. This may involve the fitting of grilles or shutters to windows (see BS 8220-3, ref. 7) and/or the use of appropriate security glazing (see BS 5544, BS 5357 and BS EN 1063, refs 8, 9 and 10 respectively). If the building is constructed with large areas of accessible, unprotected glazing then these areas should be constantly monitored. If this is not possible, then the shell of the building should not be regarded as one of the security layers.

Note: The specification and installation of security glazing should involve specialists as the technologies involved require expert knowledge. For example, bullet-resistant glazing does not necessarily give adequate protection against certain types of manual (ie non-ballistic) attack. Specifiers and suppliers must be given clear objectives based on the threat assessment.

4.3.4 Accessible glazing should also be protected by one-way vision, anti-blast films or curtains that restrict vision into the areas.

4.3.5 All accessible and vulnerable windows in the building should be kept secured shut.

4.3.6 External doors and wall apertures etc, should offer an appropriate degree of resistance, as indicated in BS 8220-3 (ref. 7).

4.3.7 Accessible doors, windows and other openings should be monitored.

4.3.8 Security doors, shutters, grilles, facades and various other products and systems for the shell of the building tested to security rating 4 or above of LPS 1175 (ref. 11) are preferred. Details of approved products are to be found in the Loss Prevention Certification Board (LPCB) Red Book Vol 1 (ref. 12).

4.3.9 If there is a need to lock the emergency exits when the building is unoccupied, there should be a robust management procedure in place to ensure that the doors are always unlocked when the building is occupied.

4.4 *Control of key areas*

4.4.1 Although the aim of a layered security plan is to prevent unauthorised access to the facilities, the IT assets should enjoy a high level of immediate security.

4.4.2 Many of the procedures recommended in Part 1: *Fire Prevention* will help in providing good security protection. Such aspects include the storing of records in lockable cabinets.

4.4.3 Hardware deemed critical, or of known high attraction to thieves, should be considered for specific protection by proprietary devices such as lock-down plates, entrapments, computer cages and computer 'safes'. It is essential to consult the manufacturer before installing these products as there may be issues concerning warranty terms, air circulation or similar matters that should be addressed. Products tested to Category 11 of LPS 1214 (ref. 13) are preferred. Details of approved products are again to be found in the LPCB Red Book.

4.4.4 Hardware and components can be marked using proprietary methods with the aim of enabling recovered property to be traced back to the owner thus acting as a deterrent to theft. Many innovative products are available, including some that have been tested to LPS 1225 (ref. 14). Details of approved products are to be found in the LPCB Red Book.

4.4.5 Electronic supervision, such as intruder alarm systems and CCTV (see section 5), can be employed very effectively to monitor sensitive zones in addition, or as an alternative, to direct surveillance.

5. **Security systems**

5.1 *Intruder alarm systems*

5.1.1 Intruder alarm systems should be installed to monitor areas in and around key buildings that are not permanently manned, including entry, exit and escape routes.

5.1.2 The method of detection (eg passive infra red, break glass should be chosen to best suit the prevailing conditions and most probable route of unauthorised entry. Installations should conform to the relevant parts of BS EN 50131 (ref. 16) or BS 4737 (ref. 17). Although parts of the latter standard have been withdrawn, it may continue to be used by sector agreement.

5.1.3 The protection of the system should be assessed; it should be noted that insurers will usually require compliance with security grade 3 of BS 50131-1 (ref. 16). Where the highest level of security is required, consideration should be given to installation of a system to grade 4 of BS 50131-1 (or BS 7042 and DD 242 (refs 18

and 19) which, although withdrawn, may continue in use for some time by sector agreement).

5.1.4 If the location is currently protected by an intruder alarm system that does not operate as a confirmed alarm system, it is strongly recommended that the design of the system is reviewed by the installer and brought into compliance with the requirements of the current edition of DD 243 (ref. 20).

5.1.5 The intruder alarm system should include the automatic transmission of alarm and fault messages to an approved alarm receiving centre (ARC), especially where appropriate personnel may not always be available, or where personnel may be subject to duress in an incident.

5.1.6 It is recommended that the transmission system takes the form of two independent paths employing different technologies. Signalling products designed to operate in this way are commonly referred to as dual path signalling systems.

5.1.7 The use of event recorders on intruder alarm control and indicating equipment should be seriously considered. These should record alarms, faults and setting/unsetting of the intruder system. Alternatively, it may be possible to log events at an alarm receiving centre.

5.2 *Closed circuit television (CCTV) systems*

5.2.1 Potentially, CCTV is a powerful security tool. However, all too often it is seen, incorrectly, as a universal panacea and there is a danger that, as a result, a lower standard of performance in other security provisions (physical barriers, intruder alarms, access controls etc) is tolerated. CCTV must be integrated as one element within the totality of measures that together build layered protection in depth.

5.2.2 The organisation needs to determine exactly what the CCTV element of the security strategy is required to provide. What is the operational requirement for the CCTV system? Is it, for example, merely required to detect the presence of persons or must it also enable the identification of persons with a high degree of certainty? Alternatively, there may be a specific purpose, such as to read vehicle number plates.

5.2.3 CCTV must be supported by observers and responders otherwise its purpose is restricted to that of deterrence or the marshalling of evidence after the event. Who and where is the observer? What will be the response? What value will it have? These questions must be addressed before the operational requirement is finally set.

5.2.4 If the risk assessment does not support provision of continuous monitoring by on-site observers, there is now a large number of remote surveillance services where incidents of a pre-determined type captured by the cameras are displayed to an operator in a remote video response centre (see BS 8418, ref. 21).

5.2.5 The effectiveness of CCTV is undermined if video recording facilities are omitted or inadequately specified. The investment made in the system will only be fully realised if state-of-the-art, high-performance Digital Video Recording (DVR) is incorporated.

5.2.6 CCTV is a complex and sophisticated technology. Once the operational requirement has been set, the services of reputable consultants and installers must be sought.

5.2.7 CCTV systems should comply with BS EN 50132 (ref. 22) and approval schemes for CCTV providers are operated by accredited certification bodies such as the National Security Inspectorate (NSI).

5.2.8 The CCTV Code of Practice to the Data Protection Act (ref. 23) sets out the management responsibilities of CCTV system owners in relation to privacy. It is vital that the user of a CCTV system that captures images of persons notifies the existence of the system to the Information Commissioner and abides by the Code which requires such things as the display of warning signs, the secure storage of images, the provision of subject access to images etc.

5.3 *Electronic access control systems*

5.3.1 In relation to electronic access control devices or systems, specifiers need to take three aspects into account when undertaking the risk assessment:

- the inherent strength required of the access point;

- the security offered by the electromagnetic locking facility;

- the sophistication required of the access control technology such as:

- recognition methodology;

- time/location zoning;

- transaction logging.

5.3.2 If an electronic access control solution is to be entertained at the outer security layers, a basic magnetic swipe card reader in conjunction with a simple electric strike or maglock to control entry may be sufficient, provided additional security is brought into play at times when a reduced level of supervision is in place.

5.3.3 As the security level increases, more sophisticated tokens (such as those incorporating an electronic chip) that can not easily be duplicated are required, perhaps in combination with a PIN pad thus requiring a 'chip and pin' approach. At these levels the locking device needs to be a heavy duty electric strike or electric lock.

5.3.4 At the very highest level of security, if the filtering process does not consist of supervision by professional security personnel at the point of entry, control might involve biometric discrimination such as fingerprint, hand geometry, face or iris recognition. At these levels, serious consideration might also need to be given to the use of a two-door interlock or a turnstile type of entry to reduce 'hit and rush' attacks and 'tailgating'.

5.3.5 Approval schemes for access control providers are operated by accredited certification bodies.

5.4 *Integrated systems*

5.4.1 Consideration should be given to the combination of the various security systems into an integrated system such that the various signals and controls available to on-site personnel are brought together coherently in a purpose-designed console. However, electronic security systems should not be integrated with other systems, unless it can be ensured that there is no loss of integrity of the security systems.

5.4.2 Priorities of actions taken should be predefined. It is recognised that fire indications and actions will receive highest priority in most cases.

5.5 *Approvals*

5.5.1 Security equipment and services should be selected from those listed in the LPCB Red Book (ref. 12), where certified approval schemes are included. Similar schemes and approvals are operated by reputable, nationally accredited test houses elsewhere in the European Union.

5.5.2 In order to satisfy the requirements of the Association of Chief Police Officers (ACPO) Policy on Police Response to Security Systems currently in force (as well as those of the insurer if an intruder alarm system is a requirement), intruder alarm systems installers and operators of alarm receiving centres must be approved by a company certificated by a UKAS-accredited certification body.

5.5.3 All installations should also meet any additional requirements of the insurers, appropriate local authority and legislation.

5.6 *Restrictions on use*

5.6.1 Certain elements of security protection – such as external CCTV cameras, security lighting, or the use of sirens – may be subject to local restrictions.

6. **Management systems**

6.1 Although the measures outlined here should deter unauthorised persons from entering offices, some equipment may need a further degree of protection against theft by intruders, visitors or even by staff. Such protection may be by additional physical means to prevent theft, or by measures to increase the undesirability of theft (ie by making resale, or disposal of stolen equipment difficult), or a combination of these factors.

6.2 Physical protection may take the following forms:

- cover locks;
- permanently fixing equipment to desks or racks;
- interconnecting equipment in such a way as to delay swift removal;
- locking equipment in secure cabinets when not in use;
- the installation of smoke producing devices which, when actuated, deny visibility within the premises out of working hours.

6.3 Methods to increase the undesirability of theft may include:

- indelibly marking equipment with the company name, logo or postcode. Any marks should incorporate a unique identification that has been registered for purposes of traceability. (Equipment manufacturers should be consulted where marking may possibly compromise warranty conditions.);
- using tamper alarm devices or similar warning systems.

6.4 Strict management procedures should be in place to control the risk or theft of portable equipment in use outside the premises. For example, where there is a danger of laptop computers being left in unattended vehicles.

6.5 Where a system is installed to release smoke in response to the actuation of a detector, the system should be manufactured, installed and maintained in accordance with BS 7939 (ref. 24).

7. **Personnel**

7.1 *Security personnel*

7.1.1 Where high levels of security are required, especially for Category 1 facilities, or where other forms of monitoring are judged to be impractical or ineffective, professional security personnel should be employed.

7.1.2 The role of security personnel should be tailored around the chosen security strategy (such as acting as a guard at a gatehouse or involved in regular surveillance of the operation).

7.1.3 Security personnel should be vetted (see BS 7858, ref. 25) and commercial services retained for on site guarding should be operated in accordance with BS 7499 (ref. 26).

7.1.4 It is recommended that only those commercial guarding services that are subject to an approval scheme operated by an accredited certification body are retained.

7.2 *Staff training*

7.2.1 All staff operating within the confines of the perimeter should have basic security training based on the security strategy.

7.2.2 All staff coming into contact with the IT operations should be trained in all necessary aspects of the security strategy, including:

- understanding of the access control principles;

- knowledge of procedures relating to authorised persons including cleaners, maintenance personnel and other visitors;

- an understanding of the incident plans relating to a breach of security and the corresponding reporting procedures;

- awareness of the need to report breaches.

7.2.3 Staff should be vigilant at all times:

- certain 'high-end' processors and servers, and the components they contain, attract determined criminals prepared to use extreme force.

- the threat to staff and security personnel must be taken into account in the risk assessment – they must not be exposed in such a way that either their welfare is at risk or they could be used, in effect, as 'hostages'.

7.2.4 The training policy should be enforced by management and regularly audited.

8.   Other considerations

8.1 Vital telecommunications, data and power cables should be protected against interference by protective trunking or metal conduit. Consideration should also be given to the protection of lines entering the building. Access points (such as junction boxes) should be equipped with tamper-detection systems. Access covers to chambers, carriageway and boxes containing critical services should be tested to LPS 1175 (ref. 11) where applicable. Details of approved products are to be found in the LPCB Red Book (ref. 12).

8.2 Mains and standby power supply equipment should be housed in security-protected areas. Air conditioning plant and other support services

vital to the operation of the facilities should be similarly assessed and protected to the same standard as the facilities themselves (Figure 1).

8.3 In addition to protection against the actions of unauthorised persons, consideration should be given to environmental and other types of hazard. The recommendations given in BS 7083 (ref. 27) should be considered.

8.4 If the facilities are susceptible to electromagnetic interference, then consideration should be given to electrical screening of the building(s) in accordance with the guidance set out in BS 7083 (ref. 27).

8.5 If there is a likelihood of attack by gas, then all ventilation inlets should be fitted with appropriate gas detectors and dampers.

9.   Loss and incident investigation

9.1 A written plan of action should be prepared detailing the procedures to be taken in the event of an incident, including a breach in security resulting in loss or damage to the facilities, or problems derived from other factors. The plan should include appropriate contacts, actions and follow up procedures.

9.2 In the event of breaches of security resulting in loss, damage or interference, a full investigation should be carried out.

9.3 The investigation should consider all aspects related to the incident covering all the layers of security protection.

9.4 The findings of the investigation should be used when taking corrective action in order to improve the security strategy.

10.   Security audits

10.1 Auditing should be carried out to ensure that the security strategy is correct and appropriate and that the resultant security measures continue to be effective. The audit should be designed to establish that:

- the physical protection measures have been installed correctly;

- the detection and alarm systems and connections are fully functional and fit for purpose;

- the access control methods operate in accordance with the designed strategy;

- appropriate personnel are fully conversant with their role as part of the security strategy.

10.2 The audit may be:

- a full inspection of security strategy involving an assessment of all the points given in 9.1;

- a full functional test of the security and access control systems;

- a test of the effectiveness of the security strategy by creating a number of test scenarios.

10.3 When the security strategy and associated methods of protection are first installed, a full audit should be undertaken.

10.4 In addition to the initial audit, regular audits should be carried out at a frequency determined by factors such as the criticality of the facilities. However, at least one audit should be carried out annually. Auditing should also be carried out after modifications to the protection systems and after security breaches.

10.5 Corrective action procedures should be implemented for problems identified as a result of auditing.

REFERENCES

1. BS EN ISO 9001: 2000: *Quality management systems. Requirements,* British Standards Institution.

2. RC3 Part 1: 2003: *Recommendations for loss prevention in electronic equipment installations: Fire prevention,* Fire Protection Association.

3. RC3 Part 3: 1992: *Recommendations for loss prevention in electronic equipment installations: Protection of data and software,* Fire Protection Association.

4. BS 6266: 2002: *Code of practice for fire protection for electronic equipment installations,* British Standards Institution.

5. BS 3621: 2004: *Thief resistant lock assemblies. Key egress,* British Standards Institution.

6. BS 1722: Fences (several parts), British Standards Institution.

7. BS 8220-3: 2004: *Guide for the security of buildings against crime. Storage, industrial and distribution premises,* British Standards Institution.

8. BS 5544: 1978: *Specification for anti-bandit glazing (glazing resistant to manual attack),* British Standards Institution.

9. BS 5357: 1995: *Code of practice for installation of security glazing,* British Standards Institution.

10. BS EN 1063: 2000: *Glass in building. Security glazing. Testing and classification of resistance against bullet attack,* British Standards Institution.

11. LPS 1175: Issue 5.3: 2005: *Requirements and testing procedures of burglary resistant building components, strongpoints and security enclosures,* Loss Prevention Certification Board.

12. Red Book Volume 1: *List of approved fire and security products and services* (published annually), Loss Prevention Certification Board.

13. LPS 1214: Issue 2.1: 2005: *Specification for testing and classifying physical protection devices for personal computers and similar equipment,* Loss Prevention Certification Board.

14. LPS 1225: Issue 3.1: 2005. *Requirements for the LPCB Approval and Listing of Asset Marking Systems,* Loss Prevention Certification Board.

15. RC3 Part 7: *Recommendations for loss prevention in electronic equipment installations: Contingency planning* (in preparation), Fire Protection Association.

16. BS EN 50131: *Alarm systems: Intrusion systems* (several parts), British Standards Institution.

17. BS 4737: *Intruder alarm systems* (several parts), British Standards Institution.

18. BS 7042: 1988: *Specification for high security intruder alarm systems in buildings.* (Withdrawn but may continue to be used in some sectors. Replaced by BS EN 50131-1: 1997.) British Standards Institution.

19. DD 242: 1998: *Code of practice for intruder alarm systems for high security areas.* (Withdrawn but may continue to be used in some sectors. Replaced by BS EN 50131-1: 1997.) British Standards Institution.

20. DD 243: 2004: *Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions. Code of practice,* British Standards Institution.

21. BS 8418: 2003: *Installation and remote monitoring of detector activated CCTV systems. Code of practice,* British Standards Institution.

22. BS EN 50132: *Alarm systems. CCTV surveillance systems for use in security applications* (several parts), British Standards Institution.

23. *CCTV Code of Practice,* 2000, Information Commissioner's Office.

24. BS 7939: 1999: *Smoke security devices. Code of practice for manufacture, installation and maintenance,* British Standards Institution.

25. BS 7858: 2004: *Security screening of individuals employed in a security environment. Code of practice,* British Standards Institution.

26. BS 7499: 2002: *Static site guarding and mobile patrol services. Code of practice,* British Standards Institution.

27. BS 7083: 1996: *Guide to the accommodation and operating environment for information technology (IT) equipment,* British Standards Institution.

FURTHER READING

1. BS EN 50133: *Alarm systems. Access control systems for use in security applications* (several parts), British Standards Institution.

2. BS EN 50136: *Alarm systems. Alarm transmission systems and equipment* (several parts), British Standards Institution.

3. BS ISO/IEC TR 13335: *Information technology. Guidelines for the management of IT security* (several parts), British Standards Institution.

4. BS ISO/IEC 17799: 2005. *Information technology. Security techniques. Code of practice for information security management,* British Standards Institution.

5. PD 6662: 2004. *Scheme for the application of European Standards for intruder and hold-up alarm systems,* British Standards Institution.

RC3
Part 2

for loss prevention in electronic equipment installations

Part 2: Security measures

Recommendations