An tÚdarás Slándála Príobháidí
The Private Security Authority

AUDITING GUIDELINES FOR PSA 67:2021

2021 EDITION

www.psa-gov.ie

Foreword

The Government of Ireland through the Private Security Services Act, 2004, established the Private Security Authority (PSA) as the national regulatory and licensing body for the private security industry. Amongst the functions of the PSA are:

- The controlling and supervising of persons providing security services and maintaining and improving standards in the provision of those services.
- Specifying standards to be observed in the provision of security services.
- Specifying qualifications or requirements for the granting of licences.

This document has been developed by the PSA for the licensing of contractors in the Access Control sector. It sets out the requirements which contractors are expected to meet and maintain in order to comply with the licensing regulations of the PSA.

The PSA would like to acknowledge the contribution of all those who participated in the development of this document and to thank the National Security Inspectorate (NSI) who provided us with permission to reproduce in full and part extracts from their Code of Practice (NCP109.2)

Contents

SCOPE 4

GENERAL 5

PART 1 – ACCESS CONTROL – SPECIFIC PROVISIONS 10

PART 2 – ACCESS CONTROL – GENERAL PROVISIONS 12

2. DEFINITIONS 12

3. GRADING OF ACCESS POINTS 14

4. LOCATION SURVEY 16

5. SYSTEM DESIGN 19

6. EQUIPMENT SELECTION AND INSTALLATION 22

7. TEST, COMMISSIONING, MAINTENANCE AND CERTIFICATION 34

8. AS FITTED DOCUMENT 39

Annex 1 41

Annex 2 42

SCOPE

This standard provides a specification for compliance with licensing by the Private Security Authority and applies to organisations seeking licences to provide electronic security services as Access Control contractors. Organisations seeking an Access Control licence will also be required to comply with PSA 74:2019 – Licensing Requirements for Security Service Providers.

The document also contains the auditing guidelines to be followed by PSA approved auditing bodies.

Organisations may choose between the European Standard ISO EN 60839-11-2 or the requirements set out in Part 2 of this document. Organisations choosing ISO EN 60839-11-2 will need to be familiar with ISO EN 60839-11-1. Organisations should read this document carefully and ensure they meet the requirements of whichever option they choose.

Organisations licensed by the Private Security Authority and those seeking a licence from the PSA must comply with this standard. Only auditing bodies approved by the PSA to audit for this standard may provide auditing services for licensing purposes.

By applying for and holding a licence, organisations agree to the sharing of information relating to this document, the contents herein and any audit (including audit reports) undertaken for the purposes of PSA licensing between the PSA and the organisation's auditing body. Where an organisation fails to comply with the requirements of this standard, the auditing body is obliged to notify the PSA.

This document is for the purpose of licensing by the PSA and should not be interpreted as meeting any other statutory obligations of an organisation. It is not a technical reference. Organisations seeking a licence in the Access Control sector must also comply with the PSA Licensing Requirements for Security Service Providers (PSA74:2019).

Only the most recent edition of the standard specified by the PSA shall apply for licensing purposes. To ascertain the edition applicable visit the PSA website, www.psa-gov.ie.

GENERAL

G.1 PSA Licensing Requirements

The PSA requirements document "*PSA Licensing Requirements And Auditing Guidelines – Electronic Security (Access Control) (PSA 67:2021)",* hereinafter referred to as PSA 67:2021, sets out the requirements to be achieved and maintained by contractors applying for a licence from the PSA in the Access Control sector.

Contractors seeking a licence in the Access Control sector from the PSA must comply with PSA 67:2021 and PSA 74:2019. A contractor's compliance with PSA 67:2021 shall be assessed against this requirements document and associated auditing guidelines by PSA approved auditing bodies

.

G.2 Approved Auditing Body

G.2.1 Certification for licensing purposes will only be accepted from auditing bodies approved by the PSA to provide auditing services for PSA 67:2021.

G.2.2 Auditing bodies shall agree in writing to be bound by these auditing guidelines and such other requirements as the PSA may require before the PSA will accept evidence of certification from them.

G.3 Audits

G.3.1 Contractors shall be subject to an audit by an approved auditing body at least once during each calendar year or at such intervals as the PSA may prescribe. The purpose of the audit is to verify compliance with PSA 67:2021.

G.3.2 The PSA may request auditing bodies to focus their audit on certain areas of an organisation's activities. Such request will be within the terms of PSA 67:2021.

G.3.3 All audits shall involve a visit to the contractor's address as stated on their PSA licence.

Where the address visited is not as stated on the licence, the auditor shall confirm that the address on the licence is the registered address of the organisation. If it is not the registered address, this should be recorded in the audit report. In such instances the address visited should be the administrative office of the organisation.

Where the address on the licence is outside of Ireland, a visit to the contractor's administrative office in Ireland shall occur. Where the overseas office has access to Irish client files, the organisation must provide a statement confirming that the requirements of PSA 67:2021are being met.

Where the administrative address is outside of Ireland, a visit to the address outside of Ireland shall take place.

Where an organisation has more than one administrative office, all records required for audit purposes should be made available at a single location on the date(s) of the audit. If this is not possible, audits should rotate between the different administrative offices of the organisation.

G.3.4 Organisations that change their legal status shall be subject to an audit. A change in legal status includes changing from a sole trader to a company, sole trader to partnership, partnership to company or unlimited company to limited company.

Where a merger of two businesses takes place and a new entity formed an audit is required.

An audit is not required where:

(a) one organisation takes over another organisation, both organisations are PSA licensed and there is no change in the legal status of the first organisation.
(b) where a change in legal status occurs and all partners, directors and shareholders of the new entity were vetted by the PSA as part of the previous entity or entities.
(c) where a sole trader changes to a company and the former sole trader is the exclusive director of the new company.

G.3.5 Organisations that change address shall be subject to a visit at their new address before their certification can be amended.

G.3.6 Audits shall be conducted in accordance with these guidelines. Where the guidelines require the recording of an action or other matter this shall be recorded in the audit report.

G.3.7 Where this document require an auditor to inspect or sample records or other documents the auditor shall select at random from a list of such records or documents

the ones to be audited. Under no circumstances shall an auditor accept records chosen or selected by the organisation.

In selecting records or documents, auditors shall select a large enough sample as to be satisfied that a representative selection has been chosen. Auditors shall, where possible, select different samples at subsequent audits.

As a minimum, the size of a sample shall equal the square root of the total records. Where the sample size exceeds 25 the Auditor may stop at 25 if satisfied that a pattern of compliance has been established from the selected sample.

The name of each sample record/document should be recorded.

G.3.8 When an organisation has successfully completed an audit they shall be issued with a certificate of compliance certifying same. Certificates shall be issued for a maximum period of 2 years.

At the same time, the auditing body shall email the PSA a copy of each new certificate (in PDF format).

G.3.9 When an audit has been completed the auditing body shall notify the PSA of same and provide a copy of the audit report to the PSA on request.

Note: Provision of a copy of the certificate of compliance/registration in accordance with clause G.3.8 shall be accepted as notification.

G.3.10 Audit reports shall be in a format agreed with the PSA.

G.3.11 Where a contractor fails to obtain full compliance to PSA 67:2021 or fails to arrange an audit for same, the auditing body shall notify the PSA.

G.4 Audit Compliance

G.4.1 Full compliance with PSA 67:2021 in accordance with **G.5** must be achieved before certification can be issued.

G.4.2 Where an organisation fails to comply with any of the requirements of this document, details of all the non-compliances shall be recorded in the audit report together

with details of the required corrective actions and the timeframe by which the corrective action is to be completed.

G.4.3 When corrective action has been completed, this should be recorded on the audit report together with details of how the corrective action was verified by the auditor, e.g. email, re-visit, etc.

G.4.4 When finalised audit reports should detail all non-compliances and corrective actions.

G.5 Audit Non-Conformances

G.5.1 Where a contractor fails to meet any of the requirements of PSA 67:2021 this shall be recorded as a non-compliance in accordance with the categories specified in these auditing guidelines. Organisations have 5 weeks from date of audit to rectify a non-conformance.

The following criteria shall apply to non-conformances.

1. Organisations shall not pass an audit where:

    a) A category 1 non-conformance is present, or
    b) 3 or more category 2 non-conformances are present, or
    c) 6 or more category 3 non-conformances are present, or
    d) A combination of 6 or more category 2 and category 3 non-conformances are present.

All non-conformances at 1) must be closed before an audit is passed.

2. An organization may pass an audit where:

    a) Less than 3 category 2 non-conformances are present, or
    b) Less than 6 category 3 non-conformances are present, or
    c) A combination, where a) is not broken, of less than 6 category 2 and category 3 non-conformances are present.

Organisations are still required to rectify all non-conformances. However, any follow up action by the auditor may be deferred until the next audit. If at the next audit a non-conformance has not been rectified, the non- conformance category shall move up a level.

3. Section 1 of the above criteria continues to apply where an organisation rectifies some of their non-conformances. An organisation may not move from section 1 to section 2 by virtue of rectifying a non-conformance.

G.5.2 Where the 4 week period referred to in G.5.1 has elapsed and an organisation has not passed an audit, the auditing body shall write to the organisation.

The organisation shall be required to rectify all outstanding matters within 14 days. They shall be advised that failure to rectify to do so within 7 days of the expiration of the 14 day timeframe, will result in their certification being withdrawn and the PSA being notified of same.

G.5.3 On receipt of notification that an organisations certification has been suspended the PSA will commence compliance action against the organisation. This action may result in the suspension or revocation of an organisations licence.

G.6 Audit Reports

G.6.1 An audit report shall be produced for each audit completed. The audit report shall include the following information:

1) The name, address and contact details of the auditing body,
2) The name of the auditor(s) who undertook the audit,
3) The date(s) of the audit(s),
4) The name, address, contact details and PSA licence number of the contractor,
5) A summary of the audit highlighting any non-conformities found.

G.6.2 A copy of the audit report shall be sent by the auditing body to the PSA upon request. The report should be submitted with 7 days of receipt of such a request.

G.7 Certification

G.7.1 All certificates for PSA 67:2021 issued by auditing bodies shall contain the organisations address as recorded on the organisations PSA licence.

PART 1 – ACCESS CONTROL – SPECIFIC PROVISIONS

1.1 Standards Required For Licensing

1.1.1 Subject to the provisions of **1.1.2**, the following standards shall apply to organisations providing a security service in the Installer of Security Equipment (Access Control) sector:

- PSA 74:2019 – Licensing Requirements For Security Service Providers
- PSA 67:2021 – Licensing Requirements For Electronic Security – Access Control (Part 1)
- I.S. EN 60839-11-2
- I.S. EN 179
- I.S. EN 1125
- I.S. EN 13637

1.1.2 An organisation who, on the 31st May 2022, is the holder of a Private Security Services Licence in the Installer of Security Equipment (Access Control) sector may opt to comply with the standards specified at Clause **1.1.1** or the standards specified at Clause **1.1.3**.

Organisations who hold a PSA Licence on the 31st May 2022 may choose to comply with the requirements of EN 60839-11-2 or Part 2 of this document.

Organisations licensed after the 31st May 2022 must comply with EN60839-11-2.

1.1.3 An organisation who meets the requirements of **1.1.2** and opts not to comply with the provisions of **1.1.1** shall be subject to the following standards when providing a security service in the Installer of Security Equipment (Access Control) sector:

- PSA 74:2019 – Licensing Requirements For Security Service Providers
- PSA 67:2021 – Licensing Requirements For Electronic Security – Access Control (Parts 1 and 2)
- I.S. EN 179
- I.S. EN 1125
- I.S. EN 13637

1.1.4 An organisation who meets the requirements of **1.1.2** and who obtains certification from an approved auditing body in accordance with the provisions of **1.1.1** shall not revert to the provisions of **1.1.3**.

1.1.5 The provisions of **1.1.3** shall cease on the 1st November 2025. From that date all organisations shall comply with the requirements of **1.1.1.**

1.2 Compliance with Standards

1.2.1 Organisations shall maintain compliance with this standard during the term of the licence. Failure to maintain compliance may result in the PSA taking action against the licensee up to and including the revocation of the licence.

The auditor shall record any instances of non-compliance with PSA 67:2021 which come to their attention in the audit report.

1.2.2 Organisations shall be subject to an audit by an approved auditing body at least once during each calendar year or at such intervals as the PSA may prescribe. The purpose of the audit is to verify compliance with the specified standards.

The auditor shall confirm that they have conducted an audit as required by the PSA and in accordance with clause 1.2.2. Non Compliance : Category 1

1.2.3 An audit report shall be completed by the approved auditing body for each audit undertaken and the organisation shall agree to the auditing body providing a copy of the report to the PSA.

1.2.4 Organisations shall give their permission to the approved auditing body to provide the PSA with information in accordance with provisions **1.2.5** and **1.2.6**.

1.2.5 Where an organisation fails to undertake or complete an audit the auditing body shall notify the PSA of the failure and the reason for same.

1.2.6 Where an organisation is found to be non-compliant with a standard the auditing body shall notify the PSA of the reason for the non-compliance and any resulting action taken against the organisation.

PART 2 – ACCESS CONTROL – GENERAL PROVISIONS

2. DEFINITIONS

2.1 **Access Control.** The control or recording of access by persons or vehicles to or within premises by means of:

a) Personal identity verification, including by means of biometrics
b) Vehicle identification
c) Numerical codes
d) Alphabetical codes
e) Access or other card management,
f) Electronic key management, or
any combination of such means.

Licensable activity includes the installation, maintenance, repair and servicing of all hardware, software (including programming), access control media, locks, door operators and closers, intercom systems or other components that form part of the access control system.

Access control media includes card, fob, numerical or digital keypad, biometrics, electronic key, remote control, mobile phone or other remote device whether installed in a domestic or commercial setting.

2.2 **Access point.** The position at which access/egress can be controlled to a door or turnstile.

2.3 **ACU.** Access control unit, a device which processes data from the reader to authorise or reject access.

2.4 **Approved Auditing Body.** An auditing body approved by the PSA to provide auditing services in respect of Access Control.

2.5 **Biometric.** A measurable, unique physiological characteristic or personal trait that is used as a credential.

2.6 **Client.** Individual or organisation retaining and maintaining a security service covered by this standard to carry out agreed services in accordance with an agreed contract or other form of oral or written agreement to provide such services.

2.7 **Contract.** Document, agreed and signed by both the service provider and the client, setting out the proposed services to be supplied and the details of the quotation, terms, conditions, responsibilities and undertakings.

2.8 **Controlled Area.** The area to which access is permitted through the presentation of a valid credential.

2.9 **Credential.** Any token or memorised information or biometric used to identify an individual to an access control system in order to verify user access.

2.10 **Data bus.** A system within a computer or device, consisting of a connector or set of wires, that provides transportation for data.

2.11 **Fail locked.** The securing of a locking mechanism at an access point in the event of identified system failures.

2.12 **Fail unlocked.** The release of a locking mechanism at an access point in the event of identified system failures.

2.13 **Organisation**. A limited or unlimited company, a partnership or sole trader providing services installing, maintaining, repairing or servicing electronic security equipment, for which a PSA Installer of Security Equipment (Access Control) licence is required.

2.14 **Private Security Authority (PSA).** The regulatory and licensing authority for the private security industry in the Republic of Ireland.

2.15 **Reader.** Equipment for the extraction of data from a token/card or other means.

2.16 **Security Service.** The provision of access control services for which a PSA licence is required.

2.17 **Site.** The premises, property, area or complex at which the service is carried out.

2.18 **Token.** A device such as an electronic key or card which is assigned to a user and which generates an authentication code which allows access.

3. GRADING OF ACCESS POINTS

3.1 Access points are graded by the requirements for successful legitimate access (see Grade I, Grade II, Grade III and Grade IV below). Grading is related to the level of security provided for each access point and the grade may change according to the time of day or night.

The Auditor shall confirm that the access system performs according to the grading level agreed between the organisation and the client and meets the requirements of clause 3.1. Non Compliance: Category 1

3.2 For each grade, access may be granted by the use of credentials permitted at higher grades, but not by the use of credentials permitted at lower grades.

The Auditor shall confirm that access is not granted through the presentation of credentials at lower grades and that the requirements of clause 3.2 are being met. Non Compliance : Category 1

3.3 Organisations shall determine the grading of each access point during the design stage, this shall be done in conjunction with the client and should be sufficient for the client's requirements.

The Auditor shall examine the design plan to confirm grading of access points are recorded and that the requirements of clause 3.2 are being met. Non Compliance : Category 1

3.4 Organisations shall include the location and grading of each of the access points making up an access control system in the system design proposal and in the as-fitted document.

a) Grade I (low risk)

At an access point to grade I, access will only be granted following:

- The input of a correct common code (or the input of a correct PIN code) of not less than 10,000 differs.

Note: 10,000 differs requires a 4 digit code number such as 1234.

b) Grade II (low to medium risk)

At an access point to grade II, access will only be granted following:

- Option A - the input of a correct PIN code of not less than 1,000,000 differs; or
- Option B - the presentation of a valid unique token to a reader.

Note: 1,000,000 differs requires a 6 digit code number such as 123456.

c) Grade III (medium to high risk)

At an access point to grade III, access will only be granted following:

- Option A - the input of a correct PIN code of not less than 10,000 differs AND the presentation of a valid unique token to a reader, or
- Option B - the presentation of a valid biometric to a reader.

d) Grade IV (high risk)

At an access point to grade IV, access will only be granted following:

- Option A - the presentation of a valid biometric to a reader AND the presentation of a valid unique token using radio frequency identification (RFID)*, comparative alternatives or
- Option B - the presentation of a valid biometric to a reader AND the presentation of a valid unique token to a reader AND the presentation of a correct PIN code of not less than 10,000 differs.

** RFID shall not rely on recognising the Chip Serial Number (CSN) only. Also the code to be read shall be stored in the memory of the card.*

The Auditor shall examine the design plan and the as-fitted document and confirm the location of each access point and its grading meet the requirements of clause 3.4.

Non Compliance : Category 1

4. LOCATION SURVEY

4.1 The organisation shall on the first visit to the site where the service is to be provided assess the clients requirements against the agreed contracted service and the physical environment.

The Auditor shall examine the location survey to ensure that the clients requirements and physical environment have been assessed in accordance with clause 4.1. Non Compliance: Category 2

4.2 Where the assessment at **4.1** identifies a weakness in any agreed contracted service this should be advised to the client and a decision sought on how to proceed. A record of this decision should be recorded before any work commences and the client advised of any revised costs.

The Auditor must be satisfied that issues identified under clause 4.1 were recorded prior to the commencement of any work and that any revised costs were notified to the client. Where no weaknesses were identified this shall be recorded in the audit report. Non Compliance : Category 2

4.3 Clients shall be provided with the manufacturers' product information and user information on any product provided to the client.

The auditor shall confirm that information has been provided to the client in accordance with Clause 4.3. Non Compliance : Category 2

4.4 Where relevant, organisations shall consult with relevant managers such as those responsible for information technology and human resources at the client's premises.

The auditor shall confirm from the location survey that relevant consultation was undertaken. Where none was undertaken, auditors shall request documented reasons why this was the case. Non Compliance : Category 2

4.5 In carrying out a location survey the following elements shall be fully taken into account and the results documented:

a) The degree of physical security and the anticipated number of users and the duty cycle of the access point to which they are fixed;

b) Environmental factors, particularly when planning to use mechanisms externally:
   - temperature
   - humidity
   - corrosion
   - vibration
   - dust and other contamination
   - physical abuse

c) The degree to which external factors will affect the level of security required such as:
   - the existing physical strength of the access point, such as doors and frames.
   - the transfer of electrical connections onto doors shall be via suitable flexible cables or other means of adequate reliability.
   - appropriate hardware shall be used where rebated and double-rebate doors are controlled.
   - necessary safety precautions shall be taken where all-glass or other special doors are controlled.
   - door closing devices shall be sufficient to close and lock the door under normal circumstances, but without undue impact upon the components of an access control system.
     Where adverse air pressure exists, organisations should provide means for relief of the air pressure.
   - doors shall be a satisfactory fit in the frame.
   - hinges, frame and fixings shall be adequate for the weight and proposed usage of a door.
     Organisations should follow manufacturers' recommendations for turnstiles and similar barriers, and their release mechanisms.
   - where manual or automatic override features are used, continuously rated releases will be required.
     Access point hardware alone may not provide sufficient physical security in some circumstances.

The degree of physical security is related to the grading of access points. An access point to a higher grade will usually require greater physical security than an access point of a lower grade.

Organisations should select the necessary locking mechanisms appropriate to the strength of a door and its frame. These should not reduce the physical strength of the access point significantly when fitting the mechanisms.

The auditor shall examine the location survey and confirm it includes all the requirements specified in Clause 4.5. Non Compliance : Category 1

5. SYSTEM DESIGN

5.1 A system design proposal which shall take into account the findings of the location survey shall be prepared and agreed with the client.

The auditor shall inspect the system design proposal document and confirm that it includes the findings of the location survey and note that the proposal has been agreed with the client in accordance with the requirements of clause 5.1.

Non Compliance: Category 1

5.2 The system design proposal shall include a site plan which shall detail the physical environment and the location of all access points.

The auditor shall inspect the system design proposal and confirm that a site plan is included and that the proposal meets the requirements of Clause 5.2.

Non Compliance: Category 1

5.3 Organisations shall ensure that access points:

- do not conflict with fire regulations
- do not restrict exit in such a way as to endanger people in an emergency
- are fitted with a 'break glass' door release on all doors leading to an exit route.

The auditor shall confirm that access points meet the requirements as specified on clause 5.3.

Non Compliance : Category 1

5.4 All installations, repairs and servicing shall be conducted in accordance with building, electrical and fire regulations.

The auditor shall obtain a declaration signed and dated by a principal of the organisation that all installations, repairs and servicing has been conducted in accordance with building, electrical and fire regulations. A copy of the declaration shall be attached to the audit report.

Where appropriate, auditors shall examine copies of any commissioned reports to ensure compliance with clause 5.4.

Non Compliance: Category 1

5.5 Any electrical installation or connection required shall comply with current national and site regulations and the electrical work shall be carried out in accordance with the National Rules for Electrical Installations (I.S 10101). Electrical work shall be carried out by technicians who are qualified to undertake such work.

The auditor shall obtain a declaration signed and dated by a principal of the organisation that all electrical installations and connections comply with all regulations and meet the requirements of the National Rules for Electrical Installations (I.S 10101). A copy of the declaration shall be attached to the audit report. The auditor shall confirm that all technicians undertaking electrical work have the required qualifications. Non Compliance: Category 1

5.6 All installations, repairs and servicing of equipment connected with escape routes shall be conducted in accordance with EN179, EN1125, EN 13637 and such other requirements as prescribed by law.

The auditor shall obtain a declaration signed and dated by a principal of the organisation confirming that all installations, repairs and servicing of equipment connected with escape routes shall be conducted in accordance with EN179, EN1125, EN 13637 and such other requirements as prescribed by law. A copy of the declaration shall be attached to the audit report. Non Compliance: Category 1

5.7 Organisations shall consider the following aspects when preparing the system design proposal:

- how access points will operate in the event of mains power failure and the period, or number of transactions, required in such circumstances;
- whether access points should fail locked or fail unlocked;
- whether secondary non-controlled locking devices should be fitted on external doors that fail unlocked;
- whether a key override is required for any critical doors to facilitate access in an emergency;
- whether ACUs will retain data in the event of data bus or power failure until the central computer or processor is operational;

- whether standby power is needed for the database (for example if held on a computer) to maintain its integrity during power failure;
- the choice of access control technology to provide an appropriate level of security for the risk to be protected;
- the choice of electronic equipment and its siting, taking into account environmental conditions and the potential for vandalism;
- the selection of access point hardware, taking into account the volume of traffic, environmental conditions and the level of physical security required;
- the number of users, access levels and time zones required, taking into account both present and predicted numbers of users and their needs;
- whether certain equipment needs to be protected against malicious damage;
- the need to site equipment such as controllers and printers in a secure area;
- the number of access points required, taking into account peak periods of use;
- whether an existing client local area network (LAN) should be used;
- ease of access to ACUs and power supplies for preventative and corrective maintenance.

The auditor shall inspect the system design proposal and confirm that it satisfies the requirements of clause 5.7.

Non Compliance : Category 1

5.8 The system design proposal shall contain the network security specifications for data protection.

The auditor shall inspect the system design proposal and confirm that it satisfies the requirements of clause 5.8.

Non Compliance : Category 1

6. EQUIPMENT SELECTION AND INSTALLATION

6.1 Except where otherwise specified, equipment shall be selected and installed to withstand the following air temperatures:

- Internally sited equipment, 0 ºC to +40 ºC
- Externally sited equipment, -20 ºC to +50 ºC

The auditor shall confirm that the equipment selected and installed meets the criteria of Clause 6.1

Non Compliance: Category 2

6.2 Equipment exposed to direct sunlight can exceed these temperatures and appropriate shielding may be required in such circumstances. When the temperature is not well maintained internally in premises, temperature may vary between -10 ºC to +40 ºC and organisations should consider using equipment suitable for external use or similar. In all cases equipment should be suitable for use in the environment in which it is installed.

The auditor shall inspect and confirm that all equipment exposed to direct sunlight meets the requirements of Clause 6.2

Non Compliance: Category 2

6.3 Organisations shall use environmental housings according to EN 60529 so as to afford appropriate protection (for example to IP54 or IP65 as applicable) where the possibility of penetration by solid objects, dust or water exists.

The auditor shall confirm that environmental housings are used in accordance with EN 60529 as specified in Clause 6.3

Non Compliance: Category 2

6.4 Credentials

Credentials may be thought of in terms of:

- something you know (code),
- something you have (token) or
- something you are (biometric).

6.4.1 The security, size and durability of a credential are dependent upon the technology used to encode it and the equipment required to read it.

The auditor shall check and ensure that the credentials in operation are compatible with the technology and equipment that they are being used in conjunction with.

Non Compliance: Category 1

6.4.2 Credential technology should be selected as appropriate to the risk being considered and the needs of the client.

The auditor shall confirm that the requirements of clause 6.4.2 have been satisfied.

Non Compliance: Category 1

6.4.3 Several types of credential are available including:

a) memorized information such as common codes and PIN codes, which are input by hand to a keypad;

b) magnetic token, including Wiegand effect;
Where magnetic tokens are powerful enough to corrupt other magnetically stored data in their immediate vicinity they should carry a printed warning to this effect.

c) infra-red token;

d) hologram token;

e) proximity tokens using technologies such as radio or induction to allow the encoded data to be read within a specified operating range;

f) biometric.

When selecting a battery powered active token the life span of the battery and the environment in which the token will be required to operate and the frequency of its use shall be taken into account.

The auditor shall check and ensure that the credentials meet the security Grade requirements and are suitable for the users and environment.
Non Compliance: Category 1

6.5 Readers

6.5.1 Readers shall be mounted:

- securely in position.
- adjacent to their access points and in positions convenient for all users to use, including those with disabilities.

The auditor shall confirm that readers are mounted and positioned in accordance with the requirements of Clause 6.5.1. Non Compliance: Category 1

6.5.2 Organisations shall provide a reader or controller and/or its associated access point hardware or a central control with the following features:

- an indication for access granted.
- variable time available for access to be made.
- tamper detection to detect access to the lock in circumstances where the lock can then be controlled from the insecure side.
- response within 2 seconds of the valid completion of the necessary data entry associated with the credential.

  Processing of more complex data such as those associated with biometric credentials may take longer than 2 seconds and this is acceptable provided the length of time is appropriate to the needs of the client.
- re-locking of an access point if it is not used within a predetermined time.

The auditor shall carry out checks to ensure that all devices comply with the requirements specified in Clause 6.5.2. Non Compliance: Category 1

6.5.3 When biometrics are used, the False Acceptance Rate (FAR) and the False Rejection Rate (FRR) should be balanced to reflect the need for security on the one hand and the need for operability on the other hand. If the FAR is high then it will be more likely that an unauthorised person will be able to gain access using their biometric. Accordingly, clients should not normally be provided with the means to adjust biometric readers as this could seriously weaken the security of the access control system.

Audit in conjunction with 6.5.4

6.5.4 If the client is provided with means to adjust biometric readers then access to the means of adjustment shall be protected against unauthorised change (for example by requiring an authorised person/manager to enter a password) and the client shall be provided with sufficient information to enable them to understand the consequences of making adjustments. For example, the client might be provided with information about the adjustments of their biometric readers that are acceptable and/or unacceptable for their security application.

The auditor shall ensure biometric readers meet the client's security and user requirements. Where the client is provided with the means to adjust FAR and FRR the auditor should ensure suitable precautions are in place to prevent unauthorised adjustment. Where biometrics are not used this shall be recorded in the audit report. Non Compliance: Category 1

6.6 Access point hardware

6.6.1 Organisations shall select access point hardware:

a) In accordance with the degree of physical security and the anticipated number of users and the duty cycle of the access point to which they are fixed;

b) With regard to the following, particularly when planning to use mechanisms externally:
- temperature
- humidity
- corrosion
- vibration
- dust and other contamination
- physical abuse

c) Taking into account the following with regard to the nature of the access point:
- the existing physical strength of the access point, such as doors and frames.
- the transfer of electrical connections onto doors shall use suitable flexible cables or other means of adequate reliability.
- appropriate hardware shall be used where rebated and double-rebate doors are controlled.
- necessary safety precautions shall be taken where all-glass or other special doors are controlled.

- door closing devices shall be sufficient to close and lock the door under normal circumstances, but without undue impact upon the components of an access control system.
  Where adverse air pressure exists, a means for relief of the air pressure should be provided.
- doors shall be a satisfactory fit in the frame.
- hinges, frame and fixings shall be adequate for the weight and proposed usage of a door.

d) Organisations shall follow manufacturers' recommendations for turnstiles and similar barriers, and their release mechanisms.

Where manual or automatic override features are used, continuously rated releases will be required.

The auditor shall carry out checks to:
6.6.1(a) - assess where access point hardware provides the necessary level of security for the Grade of access point and is suitable for the expected usage.

6.6.1(b) - ensure access point hardware is suitable for the environmental conditions.

6.6.1(c) - ensure the strength and integrity of the access point and hardware is suitable for the security Grade and usage and that installation has not compromised the structural integrity of the access point.

6.6.1(d) - ensure that manufacturer's instructions have been followed when installing access point hardware and where it is necessary to override access point hardware that continuously rated releases have been installed.

Non Compliance: Category 2

6.6.2 Access point hardware alone may not provide sufficient physical security in some circumstances.

The degree of physical security is related to the classification of access points. An access point to a higher grade will usually require greater physical security than an access point of a lower grade.

Organisations should select the necessary locking mechanisms appropriate to the strength of the door and its frame and should not reduce the physical strength of the access point significantly when fitting the mechanisms.

The auditor shall carry out checks to ensure that all devices comply with the requirements of Clause 6.62. Non Compliance: Category 2

6.6.3 The physical strength of an access point should be reinforced if this is likely to be unduly reduced by the attachment of the access control hardware. If this is not possible for any reason, the facts of the situation shall be provided in writing to the client.

The auditor shall carry out checks to ensure that devices are fitted correctly. Any deviations shall be recorded by the organisation and inspected by the auditor as having been provided to the client. Non Compliance: Category 2

6.6.4 Where access point monitoring is of critical importance, consideration should be given to monitoring the locked / unlocked state of the access point, in addition to any monitoring by means of a separate protective switch.

The auditor shall carry out checks to verify the requirements of Clause 6.6.4 are being met. Non Compliance: Category 2

6.6.5 Locking mechanisms can have two modes of operation under system failure conditions, 'failed unlocked' and 'fail locked'. Where exit is available by purely mechanical means, the fail locked mode may be acceptable but where exit is granted by electrical means, the 'fail unlocked' mode may be mandatory to meet safety legislation.

The auditor shall carry out checks to ensure that exit is possible in a system failure. Details of the checks carried out shall be recorded in the audit report.

Non Compliance: Category 2

6.6.6 In the case of a complete power failure it may be necessary to provide a key override to a critical door (or doors) with the key (or keys) kept in a safe place outside the controlled door (or doors).

Details of a key override shall be inspected by the auditor to ensure that the requirements of clause 6.6.6 have been met.

Non Compliance: Category 2

6.6.7 The suitability of any access control system shall be considered in relation to the fire risk assessment for the premises and the need for safe exit in emergency situations.

The auditor shall examine the system design proposal and the as-fitted document to verify that the system has been designed and installed with direct reference to the fire risk assessment and that safe exit facilities in emergency situations have been addressed in the design.

Non Compliance: Category 1

6.6.8 Where applicable, agreement shall be reached on what methods are to be used to release all the access points (for example green coloured single action emergency exit buttons, or break glass units, on the secure sides of access points) and these methods shall be documented in the system design proposal and the as-fitted document.

The auditor shall examine the system design proposal and the as-fitted document to ensure compliance with clause 6.6.8.

Non Compliance: Category 1

6.7 Power supplies

6.7.1 Organisations shall ensure the power supply to meet the largest load likely to be placed upon it under normal operational conditions is selected.

The auditor shall inspect the power supply used and confirm that it meets the requirements of Clause 6.7.1.

Non Compliance: Category 1

6.7.2 Any electrical installation or connection required shall comply with current national and site regulations and the electrical work shall be carried out in accordance with the National Rules for Electrical Installations (I.S 10101). Electrical work shall be carried out by technicians who are qualified to undertake such work.

The auditor shall obtain a declaration signed and dated by a principal of the organisation that all electrical installations and connections comply with all regulations and meet the requirements of the National Rules for Electrical Installations (I.S. 10101). A copy of the declaration shall be attached to the audit report.
The auditor shall confirm that all technicians undertaking electrical work have the required qualifications.

Non Compliance : Category 1

6.7.3 All equipment housings shall be clearly marked with the operating, or supplied voltage. Where ACUs use external power supplies, ACU input voltages should not exceed 50V or 75VDC unless unauthorized access to both power supply and ACU are prevented.

The auditor shall inspect all equipment housings and ensure that they are clearly marked with operating or supplied voltage and shall confirm that the requirements of Clause 6.7.3 are being met.

Non Compliance: Category 2

6.7.4 Certain release mechanisms associated with an access control system, such as those for roller shutters, may operate at mains voltage and specific electrical safety requirements will apply to these.

The auditor must confirm that all requirements of Clause 6.7.4 are satisfied
Non Compliance: Category 2

6.7.5 Where safety and security considerations do not require continued operation of a system during a mains supply failure, the public mains supply via a safety isolating transformer may be the sole supply for the system. A 'clean' source for this may be required in electrically noisy environments.

The auditor shall verify that where the public mains supply is the sole supply for the system that continued operation of the system during a supply failure is not a requirement of the client and the client is fully aware of this.

The auditor shall also verify that in these circumstances the mains supply is provided via a safety isolating transformer.

Non Compliance: Category 2

6.7.6 Organisations shall:

- locate power supply units within controlled areas and in positions secure from tampering;
- consider additional security for power supply units that incorporate fail unlock hardware;
- connect the mains power supply permanently to the access control system via a fused outlet, not by plug and socket;
- not bring extra low voltage cables into a power supply container through the same entry point as any mains cables (except where impractical to avoid doing so).

The auditor shall ensure that power supplies comply with the requirements of clause 6.7.6.

Non Compliance: Category 1

6.7.7 Where continued operation of the access control system is essential during mains supply failure, a standby power supply shall be used having the necessary capacity to support the system for not less than the minimum period as agreed with the client.

The auditor shall confirm that the requirements of Clause 6.7.7 are satisfied during a mains supply failure and that the client agreed to the requirements.

Non Compliance: Category 2

6.8 Cables

6.8.1 Where practicable, cables shall be installed within controlled areas.

The auditor shall ensure that cables are installed within the controlled areas. Where this is not practicable reasons shall be recorded.

Non Compliance: Category 2

6.8.2 Where practicable, cables shall be concealed.

The auditor shall ensure that cables are concealed. Where this is not practicable the reasons shall be recorded.

Non Compliance: Category 2

6.8.3 Where cables are exposed to possible mechanical damage or tampering, or are outside controlled areas, they shall be protected by suitable conduit, trunking, or armour.

The auditor shall confirm that cables have been installed in accordance with the requirements of Clause 6.8.3.

Non Compliance: Category 2

6.8.4 Where an access point release signal passes outside of a controlled area, metal conduit (or equivalent protection) shall be used.

The auditor shall confirm that cables have been installed in accordance with the requirements of Clause 6.8.4.

Non Compliance: Category 1

6.8.5 All interconnecting wiring shall be supported and its installation shall conform to good working practice.

The auditor shall confirm that cables have been installed in accordance with the requirements of Clause 6.8.5.

Non Compliance: Category 1

6.8.6 Any electrical installation or connection required shall comply with current national and site regulations and the electrical work shall be carried out in accordance with the National Rules for Electrical Installations (I.S 10101). Electrical work shall be carried out by technicians who are qualified to undertake such work.

The auditor shall obtain a declaration signed and dated by a principal of the organisation that all electrical installations and connections comply with all regulations and meet the requirements of the National Rules for Electrical Installations (I.S 10101). A copy of the declaration shall be attached to the audit report.

The auditor shall confirm that all technicians undertaking electrical work have the required qualifications.

Non Compliance: Category 1

6.8.7 All extra low voltage cable joints shall be made in suitable junction boxes using either soldered, crimped, or screw-terminals. Alternatively plugs and sockets can be used provided fire safety is not compromised.

The auditor shall confirm the requirements of Clause 6.8.7 have been met.

Non Compliance: Category 1

6.8.8 Extra low voltage signal cables shall not run in close proximity to mains power cables or other low or high voltage cables.

The auditor shall confirm that cables have been installed in accordance with the requirements of Clause 6.8.8.

Non Compliance: Category 1

6.8.9 Signal cables for the transmission of data or other low level signals shall be of a type and size compatible with the rate of data transfer and anticipated levels of electromagnetic interference.

The auditor shall confirm that signal cables are installed in accordance with the requirements of Clause 6.8.9.

Non Compliance: Category 1

6.8.10 Low voltage cables from both mains and standby power supplies to remote equipment shall be of sufficient rating to permit satisfactory operation of the equipment at the end of any proposed length of cable run.

The auditor shall confirm that appropriate low voltage cables are installed in accordance with the requirements of Clause 6.8.10.

Non Compliance : Category 1

6.9 Control

6.9.1 Organisations shall consider the following when selecting controls:

- operational requirements of the associated controllers;
- protection against unauthorised interference with the system database or programme;
- logging of transactions;
- annunciation of alarms;
- blocking, validation and deletion of tokens;
- database for the retention of token holder details with back-up copies of corruptible data to facilitate re-establishment of the system in the event of a failure;
- programming of access levels and time zones;
- period of operation following mains failure and/or storage of data by non-volatile means;
- ease of access for maintenance and serviceability.

The auditor shall confirm that the selection of controls is in accordance with and meets the requirements of Clause 6.91.

Non Compliance : Category 1

6.9.2 The following shall be taken into consideration when siting control equipment:

- ventilation;
- access for maintenance;
- user access for archiving;
- physical security and supervision;
- general visibility to unauthorized people of any displayed data.

The auditor shall confirm that the siting of control equipment is in accordance with clause 6.9.2.
Non Compliance : Category 1

7. TEST, COMMISSIONING, MAINTENANCE AND CERTIFICATION

7.1 Test

7.1.1 Organisations must check and test the following during commissioning and record the results which shall be signed by the person commissioning the system :

- all wiring is correctly terminated;
- alignment and operation of access point hardware and of release and closure mechanisms at each access point is correct;
- emergency release mechanisms at all the access points are in full working order;
- operation of each reader is correct;
- release time for each door is correct;
- door held open signal, if specified, is present;
- correct authorisation of access is verified by the input of appropriate data;
- access control system continues to work when mains supply disconnected (if specified).

The auditor shall inspect the commissioning results for the system and confirm that the requirements of Clause 7.1.1 are being met. Non Compliance : Category 1

7.2 Commissioning

7.2.1 At handover, organisations shall complete the following procedures, and have an acknowledgement of completion with the client's name and signature:

- provide a system log book to the client and explain how to record/report problems;
- demonstrate all aspects of the system operation to the client, including any necessary safety precautions and any standby power facilities;
- ensure that the correct documentation is given to the client to enable the system to be operated, adjusted and maintained;
- ensure that clients are advised on the importance of changing access codes including default codes and the necessary instruction provided;

- train the users in the correct operation of the system and arrange for any further training if necessary;
- for PC based systems, train the users on how to produce a system back-up and recommend that back-ups are carried out on a regular basis.
- ensure that users know the procedure for summoning assistance in the event of system malfunction;
- advise the client to establish whether personal information held within the system requires registration under the Data Protection Act.

Where an access control system is managed remotely, details of this should be included in the documentation, for example the method of control and where control is carried out.

The auditor shall inspect and confirm that the handover procedures are completed in accordance with the requirements of Clause 7.2.1. Non Compliance : Category 1

7.3 Maintenance

7.3.1 Where a client decides not to enter into a maintenance contract this shall be recorded in the as-fitted document.

The auditor shall inspect the as-fitted document to confirm that it satisfies clause 7.3.1 Non Compliance : Category 1

7.3.2 Where an organisation enters into a maintenance contract with a client it shall be documented and shall specify the schedule of maintenance agreed.

The auditor shall examine maintenance contracts to ensure that the requirements of clause 7.3.2 are being met. Non Compliance : Category 2

7.3.3 During each maintenance visit, inspection of the following, with all necessary tests, and those rectifications which are practical at the time, must be carried out:

a) the installation, location and siting of all equipment and devices against the as-fitted document,
b) the satisfactory operation of all equipment,

c) all flexible connections,
d) the normal and standby power supplies, for correct functioning,
e) the control equipment,
f) the operation of any warning device in the system,
g) the correct operation of all system security functions,
h) system application and operating software is at the correct version with any outstanding application and security patches and updates installed, subject to any software configuration controls the client may have in place.

Repairs which were not carried out during the scheduled maintenance visit shall be completed as soon as is practicable, subject to the agreement of any charges which may be applicable.

The auditor shall inspect reports from maintenance visits and ensure that all necessary tests were carried out and that all work has been completed.

Non Compliance: Category 1

7.3.4 All procedures used in the maintenance, servicing and repair of access control shall be in accordance with manufacturer's policy and instruction and meet manufacturer's specifications.

The auditor shall confirm that maintenance procedures are in accordance with clause 7.3.4

Non Compliance: Category 2

7.3.5 Any repairs or alterations to the system necessary following maintenance are to be performed in such a way as to return the system to the same level of service or better, as provided before the maintenance. Alterations shall be in accordance with the manufacturer's technical document. Where this is not possible, the client is to be advised and direction sought.

The auditor shall inspect reports from maintenance visits and ensure that all repairs or alterations to the system meet the requirements of Clause 7.3.5.

Non Compliance: Category 1

7.3.6 Any component replaced shall be of the same or increased level of security as the original component and shall not impact on the functionality or safety of the system. Where the client requests a component of a lower level of security this request shall be made in writing. Such a request shall be retained on the file of the organisation.

The auditor shall ensure that any replacement component meets the requirements of Clause 7.3.6

Non Compliance: Category 1

7.3.7 A record of all maintenance visits and of the work carried out shall be maintained.

The auditor shall inspect the maintenance record and confirm that it meets the requirements of clause 7.3.7

Non Compliance: Category 2

7.4 Certification

7.4.1 The organization shall provide the client with a certificate of conformance confirming that the access control system has been installed and tested in accordance with the as-fitted document and the date on which the next service/maintenance visit is due.

The auditor shall inspect the record of certificates of conformance and confirm that the requirements of Clause 7.4.1 are being met.

Non Compliance: Category 2

7.4.2 The certificate of conformance shall contain the following details;

a) Name of the organisation
b) PSA licence number of the organization,
c) Name of client,
d) Address at which the service was provided,
e) The nature of the service provided (installation, maintenance, repair),
f) Date service was provided,
g) Grade of system,
h) Details of any alterations, changes or other modifications to the system,
i) Date of next scheduled maintenance visit,
j) Name of person issuing certificate on behalf of organization,
k) Date on which certificate issued,
l)Date on which certificate expires,

The auditor shall confirm that certificates of conformance meet the requirements of Clause 7.4.2.

Non Compliance: Category 2

7.4.3 Modifications made to the access control system or its configuration, shall be documented and notified in writing to the client and an inspection test shall be carried out on the relevant components or parts of the system. The documentation should be appended to the as-fitted document. A new certificate of conformance which shall include the date of the next service/maintenance visit shall be issued.

The auditor shall examine the as-fitted document and confirm that any modifications made to the access control system are documented and have been notified to the client in accordance with the requirements of clause 7.4.3

Non Compliance: Category 1

7.4.4 At each service/maintenance visit the client shall receive a new certificate of conformance confirming that the access control system continues to meet the requirements of the as-fitted document including any modifications made. A new certificate of conformance which shall include the date of the next service/maintenance visit shall be issued.

The auditor shall confirm that new certificates of conformance are issued in accordance with the requirements of clause 7.4.4

Non Compliance: Category 1

8. AS FITTED DOCUMENT

8.1 Upon completion of the installation of the access control system an as-fitted document shall be produced including the following information:

- the name, address and telephone number of the controlled premises;
- the name, address and telephone number of the client;
- the name, address and telephone number of the installer;
- the location and classification of each access point and the type and location of each controller and its associated hardware (for example the type of token/reader technology);
- the type and location of power supplies;
- power supply standby periods where relevant;
- details of those access points which the client has the facility to override;
- the type and location of any warning device;
- details and settings of any pre-set or adjustable controls incorporated into the system;
- relevant documentation relating to equipment;
- relevant documentation relating to software functions;
- the number of keys, codes, tokens and so on for the system provided to the client;
- details of the methods adopted for emergency override for safe escape;
- details of maintenance schedule/requirements.

The auditor shall inspect the as-fitted document and confirm that it is in accordance with the requirements of clause 8.1.

Non Compliance: Category 1

8.2 The as-fitted document shall be agreed with the client and a copy provided to the client.

The auditor shall confirm that the requirements of clause 8.2 have been met.

Non Compliance: Category 2

8.3 Some of the information required for the as-fitted document may be provided in the form of a diagram of the installed system.

The auditor shall inspect the as-fitted document and confirm if the requirements of clause 8.3

Non Compliance: Category 2

8.4 The client should be advised to keep all documentation for the access control system in a place where access is restricted to authorized people.

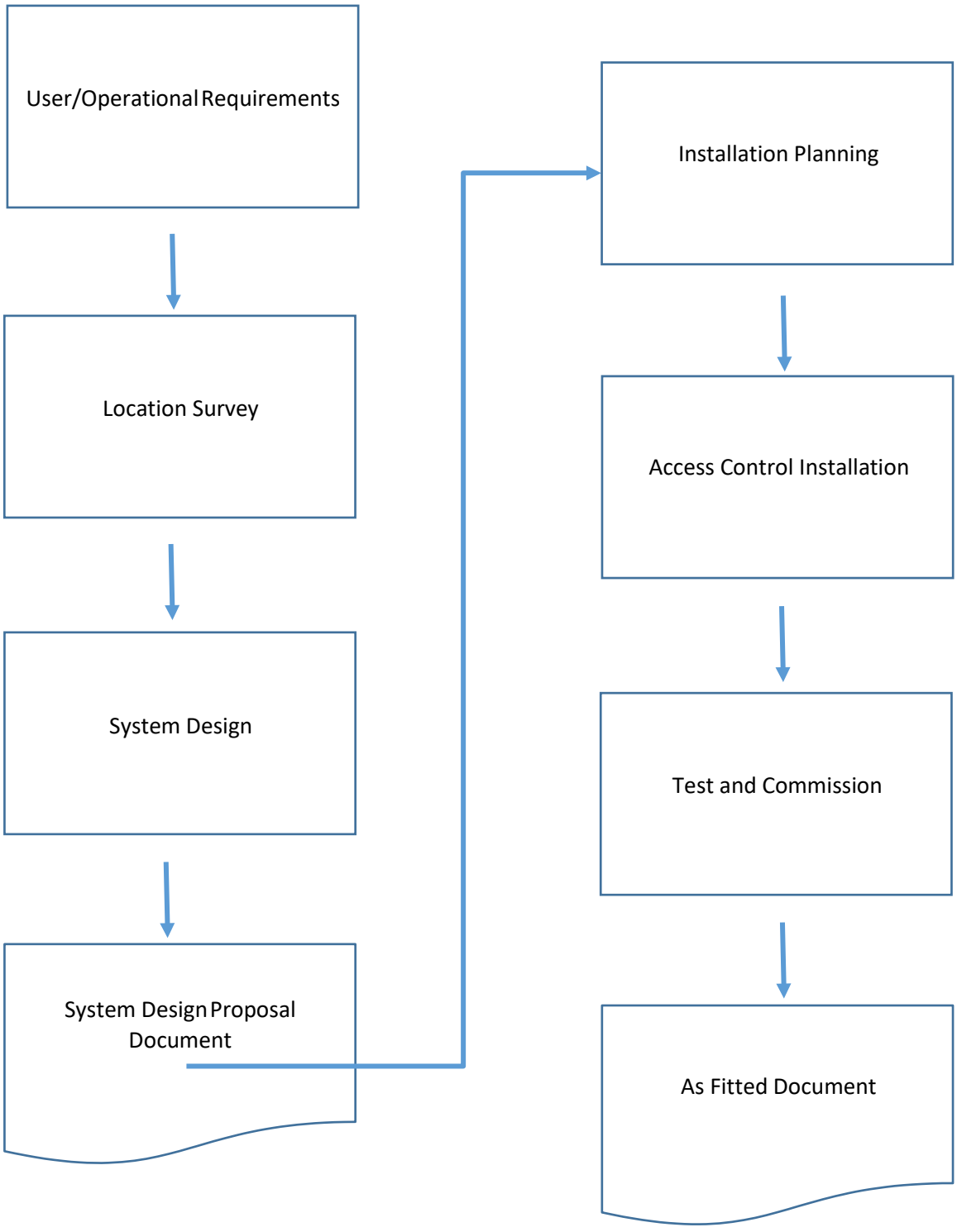
The auditor shall confirm that the requirements of clause 8.4 have been satisfied. Non Compliance: Category 2

8.5 For PC based access control systems, the software media may be handed over to the client for safe keeping on site for use during service visits if required. A back-up of the initial system configuration (which may also include a copy of the database records) may also be handed over to the client for system recovery if necessary.

The auditor shall confirm if the requirements of clause 8.5 are being met. Non Compliance: Category 2

Annex 1

Flow Chart of Access Control Installations



Annex 2

Information to be included in the System Design Proposal

A system design proposal shall be prepared for the attention of the client or specifier (or his or her agent) of the Access Control system. The proposal shall include all the information necessary to enable the client or specifier to ensure the Access Control system is appropriate for the application. The information provided in the proposal shall include the following.

Client details
The name, address and the trading name (if different from the name of the client) and any other information necessary to clearly identify the client.

Organisation details
The name, address and trading name (if a trading name is used) of the organisation shall be included along with any other information necessary for the client to identify and/or contact the organisation. Headed company stationery with organisation details is acceptable in this regard.

Supervised area details
The name and address of the supervised area shall be included if different from the address of the client. This shall also include a description of the supervised area and an indication of what the area is used for.

Schedule of equipment
A schedule of the type and location of operational equipment (in words and/or diagrammatic form) shall be included.

Control
Details of the proposed control equipment shall be included.

Legislation
Details of any claims of compliance of the system components to any local or National legislation shall be included.

Annex 2(cont'd)

Standards

Details of any claims of compliance of the system components to any National or European Standards shall be included.

Other regulations

Details of any claims of compliance of systems components to any other regulations shall be included.

Certification

Details of any claims for certification of the system components shall be included.

Maintenance

The system design proposal shall include recommendations for the scheduled maintenance of the Access Control system or individual components including details of the frequency of any maintenance visits and a list of the work to be carried out during each visit.

When serviced the Access Control system shall be inspected, tested and adjusted to ensure correct operation in line with the functional requirements of the Access Control system as outlined in the As Fitted Document.

Care should be taken to ensure that the equipment is properly reinstated after testing. All maintenance shall be carried out in reference to the manufacturer's recommendations.

Repair

Details of the proposed repair service to be provided including contact names and telephone numbers.