

Auditing Guidelines For Enforcement Guard Contractors

2024 EDITION

PSA 91:2023
June 2023

www.psa.gov.ie

Contents

1.	AUDITING GUIDELINES	3
2.	GENERAL	4
2.1	PSA Licensing Requirements	4
2.2	Audits	4
2.3	Absence of Contracts	6
2.4	Audit Compliance	6
2.5	Audit Non-Conformances	6
2.6	Audit Reports	8
2.7	Certification	8
3.	ORGANISATION	9
3.1	Ownership	9
3.2	Finances	12
3.3	Insurance	14
3.4	Premises	15
3.5	Organisation Information	16
3.6	Quotations in pursuance of Contracts or Business	18
3.7	Compliance with Legislation	18
4.	STAFFING	21
4.1	Selection and Pre-Employment Screening	21
4.2	Terms of Employment	33
4.3	Code of Conduct	34
4.4	Licence Card	35
4.5	Uniform	36
5.	TRAINING	39
5.1	Training Policy and Responsibility	39
5.2	Induction Training	40
5.3	Specialist Training	40
5.4	Refresher Training	41
5.5	Supervisory and Management Training	41
5.6	Training Records	42
6.	OPERATIONS	44
6.1	Risk Assessments	44
6.2	Times and Hours	49
6.3	Mode of entry	49
6.4	Goods	50
6.5	Vulnerable situations	51
6.6	Enforcement Manager	51
6.7	Command and Control Systems	53
6.8	Incident Reporting	55
6.9	Threats and Violence	57
6.10	Operations Records	59
6.11	Assignment Instructions	60
6.12	Security of Information and Access Media	62
6.13	Vehicles and Equipment	65
7.	COMPLIANCE WITH PSA LICENSING	67
7.1	Compliance with Standards	67
7.2	PSA Licensing Requirements	68
ANNEX A	Screening Forms	70
ANNEX B	Risk Assessment Guidelines	74
ANNEX C	Cash Flow Template	84
Annex D	Audit Report	85

Auditing Guidelines

The Government of Ireland through the Private Security Services Act, 2004, **as amended**, established the Private Security Authority (PSA) as the national regulatory and licensing body for the private security industry. The PSA has prescribed PSA Licensing Requirements – **Enforcement Guards (PSA91:2023)** as the standard to be observed by contractors in the **Enforcement Guard** sector.

These guidelines set out the auditing requirements to be followed when auditing organisations for **Enforcement Guard (PSA91:2023)** certification. The guidelines should be read in conjunction with the PSA requirements document, PSA Licensing Requirements - **Enforcement Guards (PSA91:2023)**.

For ease of use, this document includes the relevant clause from PSA91:2023 with the auditing guidelines.

The guidelines will be reviewed on a regular basis and updated versions will be made available on our website, www.psa.gov.ie.

2. GENERAL

2.1 PSA Licensing Requirements

The PSA requirements document “*PSA Licensing Requirements – Enforcement Guards (PSA 91:2023)*”, hereinafter referred to as PSA 91:2023, sets out the requirements to be achieved and maintained by contractors applying for a licence from the PSA in the enforcement guard sector.

Contractors seeking a licence from the PSA must comply with PSA 91:2023. A contractor’s compliance shall be assessed against the requirements document by auditors in accordance with these guidelines.

2.2 Audits

2.2.1 Contractors shall be subject to an audit 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 91:2023.

2.2.2 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 91:2023 are 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.

2.2.3 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.

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

2.2.5 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.

2.2.6 Where PSA 91:2023 or these guidelines 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. Inspectors 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.

2.2.7 When an organisation has successfully completed an audit they shall be issued with a certificate of compliance or letter of approval certifying same. Certificates or letters of approval shall be issued for a maximum period of 2 years.

At the same time, the auditor shall email the PSA a copy of each new certificate/approval letter (in PDF format).

2.2.8 When an audit has been completed the auditor shall notify the PSA of same and provide a copy of the audit report on request.

Note: Provision of a copy of the certificate of compliance/registration in accordance with

clause 2.2.8 shall be accepted as notification.

2.2.9 Audit reports shall be in the format set out in **Annex D**.

2.2.10 Where a contractor fails to obtain full compliance to PSA 91:2023 or fails to arrange an audit for same, the auditor shall notify the PSA.

2.3 Absence of Contracts

Where an organisation who holds a PSA licence is unable to complete an audit because of an absence of contracts the requirements of AB 3:2023 shall come into operation.

2.4 Audit Compliance

2.4.1 Full compliance with PSA 91:2023 in accordance with 2.2 must be achieved before certification can be issued.

2.4.2 Where an organisation fails to comply with any of the requirements of the requirements 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.

2.4.3 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 inspector, e.g. email, re-visit, etc.

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

2.5 Audit Non-Conformances

2.5.1 Where a contractor fails to meet any of the requirements of PSA 91:2023 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.

- a. Organisations shall not pass an audit where:
 - A category 1 non-conformance is present, or

- 3 or more category 2 non-conformances are present, or
- 6 or more category 3 non-conformances are present, or
- 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.

b. An organisation may pass an audit where:

- Less than 3 category 2 non-conformances are present, or
- Less than 6 category 3 non-conformances are present, or
- 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.

c. 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.

2.5.2 Where the 5 week period referred to in 2.6.1 has elapsed and an organisation has not passed an audit, the inspector 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 suspended for a period of 3 months and the PSA's licensing division being notified of same.

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

2.6 Audit Reports

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

- The name of the auditor(s) who undertook the audit,
- The date(s) of the audit(s),
- The name, address, contact details and PSA licence number of the contractor,
- A summary of the audit highlighting any non-conformities found.
- Update report on screening and training records reviewed to date (see Annex A).

2.6.2 A copy of the audit report shall be sent by the auditor to the PSA upon request. The report should be submitted with 14 days of receipt of such a request.

2.7 Certification

2.7.1 All certificates/letters of approval for PSA 91:2023 issued by the auditor shall contain the organisation's address as recorded on the organisation's PSA licence.

03— Organisation



3. ORGANISATION

3.1 Ownership

3.1.1 Ownership and management of the organisation shall be clearly stated in writing. The directors, company secretary and all individuals who have a shareholding or control of more than 5% of the organisation shall be properly identified.

The name and contact details of each person who owns part of the organisation or who has control over the organisation shall be recorded in the audit report together with the name and contact details of the organisation's management.

Auditors shall refer to reliable sources of information such as the CRO. Where the company is a PLC details of shareholdings are not required. However, details of senior management responsible for the licensable sectors should be recorded in the audit report.

Non Compliance: Category 3

3.1.2 The names of all directors of the organisation shall be properly recorded in the Companies Registration Office, and shall be as named. Screening of all directors shall be carried out as set out in section 4.1. A record of this screening shall be recorded and held on file, these records shall be available to an authorised official.

The auditor shall examine the records to ensure compliance. The audit report shall confirm that the details provided correspond to the director details recorded with the Companies Registration Office, a copy should be included in the report.

A record of screening of each individual must be examined.

Non Compliance: Category 3

3.1.3 Screening shall include details of employment and current and previous directorships, shareholdings etc.

The results of the screening of principals and directors including the company secretary shall be audited for compliance with screening requirements. The audit report shall confirm that screening requirements were met.

Non Compliance: Category 1

3.1.4 An organisation applying for a licence must provide evidence that they possess

the competence to provide a security service. Competence may be demonstrated by the following means:

- a) 5 years continuous experience in the sector for which a licence is sought within the previous 8 years, or
- b) possession of a PSA contractor licence in the event security, security guarding or door supervision sectors for the previous 5 years, or
- c) such other means as may be approved by the PSA.

Note: Where an organisation is a body corporate, at least one director should demonstrate that they possess the required competence. Where an organisation is a partnership, at least one partner should demonstrate that they possess the required competence, all sole traders should demonstrate that they possess the required competence.

The auditor shall examine the verified evidence of 5 years continuous experience of providing a security service or possession of a PSA contractor licence in the required sectors for 5 years. Where an organisation does not meet the requirements of 3.1.4 a) or 3.1.4 b) it must first have received approval by the PSA that the other means are satisfactory.

Non Compliance: Category 1

- 3.1.5 Details of former businesses, directorships, partnerships, or sole trades etc. of directors shall be recorded and held on file, these records shall be available to an authorised official.

The organisation shall confirm to the auditor details of former businesses, directorships, partnerships or sole trades of directors and evidence of such records shall be made available to the auditor.

Non Compliance: Category 3

- 3.1.6 Details of any bankruptcy whether discharged or undischarged of a principal or director of the organisation shall be held on file and shall be disclosed to a client on request.

The organisation shall confirm to the auditor if any principal or director is or has been a bankrupt. If confirmed, details of the bankruptcy shall be inspected in the organisation's files and the name of the person involved and the period of the bankruptcy recorded in the audit report.

Non Compliance: Category 3

- 3.1.7 Where a principal has a beneficial interest in another organisation subject to licensing by the PSA, a declaration of that interest shall be made.

The organisation shall confirm to the auditor if any of the principals hold a beneficial interest in any organisations subject to licensing by the PSA. If confirmed the details shall be inspected and the names, contact details of such principals and details of the other licensed entity shall be recorded.

Non Compliance: Category 3

- 3.1.8 All principals shall sign a declaration providing details of any person who is a beneficiary of the organisation or any person that may hold a major interest in the organisation and who has not been identified at section **3.1.1** or **3.1.2**.

The organisation shall confirm to the auditor the name and contact details of any person who is a beneficiary of the organisation or any person that may hold a material interest in the organisation and who has not been identified at **3.1.1** or **3.1.2**. The details of such persons shall be provided to the auditor in the form of a declaration and shall be attached to the audit report.

Where none is declared, a signed written declaration must be provided.

Non Compliance: Category 3

- 3.1.9 The principal shall ensure that an up to date organisation chart is prepared which details all the persons involved and all persons proposed to be involved in the organisation. The chart shall include details of any third party who will provide additional services to or for the organisation such as sales, payroll and accounts.

The organisation shall provide the auditor with a detailed organisation chart showing all persons involved in the management or operation of the business and to include all persons and third parties, including consultants, providing regular ancillary services to the business such as sales, client liaison, consultancy services, payroll, training and account services.

In the case of services provided by third parties it is sufficient to record the name of the third party on the organisation chart. A copy of the organisation chart should be attached to the audit report.

Non Compliance: Category 3

- 3.1.10 All directors, management, supervisory and operational staff shall hold a current PSA employee licence where they are carrying out an activity that is subject to PSA licensing.

The auditor shall be provided with the name and PSA licence number of all operational directors, supervisory and management staff who undertake licensable activities. These details should be recorded in the audit report.

Non Compliance: Category 1

3.2 Finances

- 3.2.1 The organisation shall be tax compliant. Holders of eTax Clearance certificates shall provide the Tax Reference Number (TRN) and Tax Clearance Access Number (TCAN) and allow Authorised Officials access to Revenue.ie to allow verification.

Where access to the Revenue On-line System (ROS) is carried out by an agent, organisations shall provide in addition to the above an up to date 'hard copy' of the certificate, the date it was printed showing at the bottom of the document.

The auditor shall inspect the organisation's tax clearance record through Revenue.ie and verify that it relates to the organisation and is valid. The following details from the tax clearance certificate shall be recorded in the audit report:

- ┆ Date Accessed
- ┆ Tax Clearance Status

Companies based outside of the State who are not obliged to register for tax may produce a 'hard copy' Tax Clearance Cert.

Non Compliance: Category 1

3.2.2 Loans from directors and/or shareholders shall be loan capital, subordinated to all other creditors.

The organisation shall confirm in writing to the auditor whether or not there are any loans to the organisation from the directors and/or shareholders. The auditor shall verify that all such loans are recorded in the organisation's accounts as loan capital. The following details shall be recorded in the audit report:

- ┆ Date of loan
- ┆ Amount of loan
- ┆ Who the loan is from
- ┆ Amount of any repayments made
- ┆ Date of repayments
- ┆ Amount outstanding at the time of audit

Non Compliance: Category 2

3.2.3 Each organisation shall produce and make available, a projected cash flow statement for the next 12 months upon request by authorised officials. For new organisations, a cash flow forecast for the first 12 months of business shall be provided. (see **Annex C** for suggested format).

Where requested by the PSA, the auditor shall inspect the organisations cash flow plan and satisfy themselves that the projections and figures underpinning the plan are reasonable, and are in line with a company within the industry.
A copy shall be attached to the audit report.

Non Compliance: Category 2

3.3 Insurance

3.3.1 Organisations are required to hold insurance relevant to the nature of the business undertaken. This includes, where the service provided dictates, but is not limited to cover for the following:

- Employer liability and public liability
- Motor insurance
- Professional indemnity
- Deliberate act
- Fidelity
- Defamation
- Efficacy
- Loss of keys and consequential loss of keys
- Wrongful arrest
- Personal Attack
- Death in Service

The auditor shall inspect the organisation's insurance and verify insurance cover is in place. The audit report shall record the maximum liability in each area.

- └ Employer liability and public liability
- └ Motor insurance
- └ Professional Indemnity
- └ Deliberate Act
- └ Fidelity
- └ Defamation
- └ Efficacy
- └ Loss of keys and consequential loss of keys
- └ Wrongful arrest
- └ Personal Attack
- └ Death in service

Non Compliance: Category 1

3.3.2 The organisation shall have sufficient funds to cover three times the value of the insurance excess amount of their insurance policy. These funds shall be held in a bank account separate to the organisation's operational account.

The organisation shall provide the auditor with a signed declaration advising of the amount held in a separate operational bank account and confirming that it is equivalent to three times the value of the insurance excess amount of their insurance policy. The declaration shall be attached to the audit report.

Non Compliance: Category 1

- 3.3.3 Organisations shall not self-insure in whole or in part for the services they provide.

The organisation shall provide the auditor with a signed declaration confirming that the organisation does not self-insure in whole or in part for the services they provide.

Non Compliance: Category 1

3.4 Premises

- 3.4.1 The organisation shall have an administrative office where records, together with all professional and business documents, certificates, correspondence and files necessary to the proper conduct of business shall be kept in a secure confidential manner.

The auditor shall visit the administrative office of the organisation and confirm that all records, business documents, certificates, correspondence and files necessary for the proper conduct of business are kept in a secure confidential manner.

Non Compliance: Category 2

- 3.4.2 Any administrative office covered by **3.4.1** above shall be protected by an intruder alarm system installed and maintained in accordance with prevailing PSA requirements. The organisation shall keep a written record containing the name, address, contact number and PSA licence number of the intruder alarm installer as well as details of the maintenance and service history.

3.4.3 The alarm shall be remotely monitored by:

- a) a PSA licensed Alarm Monitoring Centre. (The organisation shall keep a written record of the name, address, contact number and PSA licence number of the PSA licensed Alarm Monitoring Centre providing this service) or,
- b) such other means as may be approved by the PSA

The auditor shall confirm that the alarm is remotely monitored by one of the following:

- ┆ PSA licensed monitoring centre. The auditor shall inspect the organisation's written record of the name, address and contact number of the monitoring centre providing this service. The name and PSA licence number of the monitoring centre shall be recorded in the audit report, or
- ┆ Monitoring centre, where the administrative office is located outside of Ireland, certified to EN 50518/BS 5979 or equivalent standard recognised by the PSA.

Non Compliance: Category 2

3.5 Organisation Information

3.5.1 The organisation shall clearly state its PSA licence number(s) for all categories for which it is licensed to provide services on all organisational letterheads, contracts and advertising and promotional documents and/or media.

The auditor shall inspect the organisation's letterheads, advertising, promotional documentation and contracts and confirm the presence of the organisation's PSA licence number(s) for all categories for which the organisation is licensed.

The auditor shall confirm that advertising and media material both visual and audio, states that the organisation is licensed by the Private Security Authority.

**Non Compliance: Category 1 for engaging in unlicensed activity.
Category 3 for breaches in advertising and promotional activity.**

3.5.2 The provision of contracts to clients is mandatory and contracts shall include the following minimum provisions in respect of the organisation providing the service:

- a) Total costing (including VAT) for the service to be provided and the arrangements for payment.
- b) Obligations to the client, with references to any specialist advice to be provided (survey), contracted duties (assignment instructions) and compliance with industry standards or codes of practice.
- c) Agreement on conditions for the use of subcontractors, where applicable.
- d) Period of the contract and requirements for its termination with specific reference to any exclusions, penalty clauses or other restrictions.
- e) Safety statement.
- f) Details of complaints procedures and complaints management procedures.
- g) The scope of the service to be provided.

The auditor shall choose a number of contracts to confirm this requirement is met.

If the organisation provides licensable activities in a sector for which it does not hold a licence this shall be brought to the attention of the organisation and the PSA.

The auditor shall record in the report the quantity of contracts selected and the reference number.

Non Compliance: Category 2

3.5.3 The agreed contract shall be signed by a principal of the organisation and of the client and a copy retained by each. Where the client chooses not to sign or return a contract the organisation shall maintain evidence on file of postage (registered) or delivery of the contract to the client and any subsequent correspondence.

The auditor shall confirm that contracts are signed by a principal of the organisation and by the client and a copy retained by the organisation. Where the client has not signed the contract the auditor shall confirm that evidence of postage of the contract to the client by registered post/e-mail delivery is available.

Non Compliance: Category 2

3.5.4 Organisations engaging subcontractors for any licensable activity in the provision of services shall require the subcontractor to provide evidence of compliance with PSA standards. In addition, subcontractors shall provide evidence of holding the required, current valid PSA licence before the services of that subcontractor are engaged.

The auditor shall examine the records in relation to subcontractors and confirm that each contractor held a PSA licence when a contract was awarded.

The auditor shall record the PSA licence number of each subcontractor or record 'none' where no subcontractors were engaged.

Non Compliance: Category 1

3.6 Quotations in pursuance of Contracts or Business

3.6.1 Organisations shall provide each prospective client with a clear written quotation which shall, if agreed and accepted, form part of the contract.

The auditor shall select at random a sample of written quotations and confirm that they comply with the requirements of clauses 3.6.1 and 3.6.2 of PSA 91:2023.

The auditor shall record their findings together with the number and ratio of quotations selected in the report.

Non Compliance: Category 2

3.6.2 The documented quotation shall include the total cost for the service and method(s) of payment.

The auditor shall record their findings in the audit report, based on the sample of records selected at 3.6.1.

Non Compliance: Category 2

3.7 Compliance with Legislation

3.7.1 The organisation shall have and make available to a client or potential client a statement signed and dated by a principal of the organisation, of its compliance

with all relevant legislation and shall state specifically its compliance, where relevant, with the following:

- Safety, Health and Welfare at Work Act(s).
- Organisation of Working Time Act(s).
- Private Security Services Acts.
- Taxation and Social Welfare Acts.
- Payment of Wages Act.
- Immigration Acts.
- Data Protection Acts.
- Irish Human Rights and Equality Commission Act 2014.

Relevant verification shall be available to all statutory bodies and their agents, including but not limited to:

- The Private Security Authority.
- Auditors appointed by the Private Security Authority.

The organisation shall provide the auditor with a current statement, signed by a principal of the organisation, confirming compliance with all relevant legislation and shall state specifically its compliance, where relevant, with the following:

- ┆ Safety, Health and Welfare at Work Act(s).
- ┆ Organisation of Working Time Act(s).
- ┆ Private Security Services Acts.
- ┆ Taxation and Social Welfare Acts.
- ┆ Payment of Wages Act.
- ┆ Immigration Acts.
- ┆ Data Protection Acts
- ┆ Irish Human Rights and Equality Commission Act 2014

The statement shall be dated within 2 weeks prior to the audit date and shall be attached to the audit report.

Health, Safety and Welfare at Work Act(s): Organisations are required to keep recorded evidence that each employee is aware of Health & Safety Policy.

Organisation of Working Time Act(s): A number of employee records (timesheets/rosters) should be inspected to ascertain the number of hours worked over a period of time.

Non Compliance: Category 2

3.7.2 The organisation shall appoint a member of the management team responsible for ensuring that the organisation at all times operates in accordance with the provisions of the Private Security Services Act, regulations thereunder and the standards prescribed for licensing.

The organisation shall provide the auditor with the name and role within the organisation of the person responsible.

The name and role shall be recorded in the audit report.

Non Compliance: Category 2

04—
Staffing



4. STAFFING

4.1 Selection and Pre-Employment Screening

4.1.1 General

4.1.1.1 The organisation shall carry out detailed pre-employment enquiries to ensure that all personnel are competent and of good character.

The auditor shall inspect a selection of the organisation's pre-employment records to confirm enquiries in respect of competency and good character have been completed.

The auditor shall record their findings together with the number and ratio of records selected in the report.

Non Compliance: Category 3

4.1.1.2 All persons offered employment by the organisation for posts involving services subject to licensing by the PSA or posts involving access to details of clients shall be screened.

The auditor shall inspect the organisation's pre-employment records and confirm the required screening of all relevant persons offered employment.

In addition to persons providing licensable activities, relevant persons includes any person who will have access to details of security duties, call handling or security services provided to clients as well as any person supervising relevant persons.

When selecting records for inspection auditors should not limit the selection to persons providing licensable activities. Persons in all relevant employment areas should be identified and included.

The auditor shall record their findings together with the number and ratio of records selected in the report.

Non Compliance: Category1

4.1.1.3 A personnel file shall be established for each person subject to screening.

The auditor shall confirm the existence of personnel files for persons subject to screening and shall confirm that records previously examined continue to be maintained. The personnel file checklist at **Annex D** shall be completed.

The auditor shall record their findings together with the number and ratio of records selected in the report.

Non Compliance: Category 1

4.1.1.4 All applicants for relevant employment shall be required to provide the following:

- a) An acknowledgement signed and dated by the applicant, that misrepresentation, or failure to disclose material facts may constitute grounds for dismissal.
- b) A signed statement authorising an approach to former employers, State institutions, personal referees, etc., for verification of their career and employment record (see **Annex A, Form 1** for a suggested format).

The auditor shall inspect a selection of personnel files and confirm that they include the required statement of authorisation and the acknowledgement document signed and dated by employees in accordance with PSA requirements.

The auditor shall record their findings together with the number and ratio of records selected in the report.

Non Compliance: Category 2

4.1.1.5 No applicant shall be offered relevant employment unless they hold a PSA Licence and until screening is completed

The auditor shall confirm that the organisation meets this requirement. The PSA Licence number and confirmation that screening has been completed for the personnel files inspected shall be recorded in the report.

Non Compliance: Category 1

4.1.1.6 Probationary employment should be for a period of six months and in no case shall exceed a period of nine months.

The auditor shall confirm that, in the case of probationary employment, the time period has not exceeded 9 months.

The auditor shall record their findings together with the number and ratio of records selected in the report.

Non Compliance: Category 3

- 4.1.1.7 Certified copies of all relevant personnel and screening documentation shall be held on file.

The auditor will inspect a selection of personnel files to verify the certified copies of relevant personnel and screening documentation held.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 1

- 4.1.1.8 The requirements in Section 4.1 shall be applied equally to full-time and to part-time employees and at all levels of seniority, including directors.

The auditor will include in the inspection, the personnel files of part-time employees and directors and confirm that such files include completed screening records.

Non Compliance: Category 1

- 4.1.1.9 The relevant provisions of these requirements shall apply to all ancillary staff including those employed on a temporary basis.

The auditor will include in the inspection the personnel files of temporary and ancillary staff engaged in relevant employment and confirm that such files include completed screening records.

Non Compliance: Category 1

4.1.1.10 The screening period shall not be less than five years or from school leaving, whichever is the shorter duration.

The auditor shall confirm that screening periods are in accordance with clause 4.1.1.10 of PSA 91:2023. The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 1

4.1.1.11 Persons employed for security duties as Enforcement Guard personnel shall not be less than 18 years of age.

The organisation shall provide a signed declaration confirming that all enforcement guard personnel are 18 years of age or over.

Non Compliance: Category 2

4.1.1.12 Persons beyond sixty-six years of age employed for security duties as Enforcement Guard personnel shall be required to undergo an annual medical examination to ensure their fitness for the duties to which they may be assigned.

The auditor shall confirm that personnel aged sixty-six years of age employed for security duties as an enforcement guard meet the requirements of 4.1.1.12.

Non Compliance: Category 2

4.1.1.13 The employee shall be classed as 'employed subject to satisfactory screening' whilst screening is continuing and shall be subject to a strict system of monitoring and supervision during this period.

The auditor shall inspect the organisations provisional employment procedures to ensure the satisfactory monitoring and supervision of such personnel during the provisional period of employment.

Non Compliance: Category 1

4.1.1.14 Screening covering the whole of the screening period shall be completed no later than ten weeks after employment has commenced.

The auditor shall inspect a selection of personnel files and confirm that screening has been completed within the time frame required in clause 4.1.1.14 of PSA 91:2023.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 1

4.1.1.15 Full screening for the period covered under **4.1.1.10** above shall apply. Screening for a shorter period can be carried out where:

- a) an employee or director holds a current PSA licence, and
- b) has, immediately prior to the commencement of this employment, been employed by another licensed security provider, and
- c) the previous employer referred to in b) has carried out the full screening requirements within the preceding five years.

Where a), b) and c) above apply, screening shall be carried out from the date the screening by the previous employer had been conducted until the commencement of this employment.

The auditor shall confirm that where screening for a shorter period has occurred it is carried out in accordance with clause 4.1.1.15 of PSA 91:2023. The auditor shall record their findings together with the number of records examined, in the report.

Non Compliance: Category 1

4.1.1.16 Where the provisions of **4.1.1.15** apply, the previous licensed employer shall, upon receipt of a written request by an immediately subsequent employer covered by this standard, forward those parts of the employee's personnel file relating to details of screening and training undertaken by the previous employer. Any requested details in relation to other parts of the personnel file held by the previous employer shall be released only where the employee gives permission in writing to the previous employer to release such details.

Where applicable, auditors shall confirm that employees have provided permissions to former employers as required in accordance with clause 4.1.1.16 of PSA 91:2023

Non Compliance: Category 1

4.1.2 Pre-Employment Interview

4.1.2.1 Prior to the interview the applicant shall submit a curriculum vitae or other documentation containing:

- a) A list of the applicant's previous employers along with dates worked for each employer.
- b) Contact details for previous employers listed.
- c) Details of relevant training, qualifications and experience together with supporting documentation.
- d) Periods of unemployment.
- e) Applicant's current place of residence.

The auditor shall select a number of personnel files and inspect the pre-employment interview record in order to confirm the inclusion of the following documentation:

- Details of previous employers and employment dates,
- Contact details for previous employers,
- Dates of relevant Training and Experience,
- Applicant's current address,
- Dates of unemployment.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 2

4.1.2.2 A personal interview of a duration sufficient to assess the following shall be conducted by the organisation:

- a) The general ability, both physical and intellectual of the applicant and the overall demeanour of the applicant.
- b) Verification of personal documents e.g. birth certificate, driving licence, passport, service records, current security licence, work visa etc.

- c) The applicant's previous employment history and experience, including reason(s) for leaving previous employments.
- d) Verification of qualifications/training.
- e) The level of occupational fluency in respect of reading, writing and oral communication in the English language.
- f) The applicant's experience, if any, in the security industry.

The auditor shall select a number of personnel files in order to confirm that the personal interview has been carried out and the requirements have been met.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 2

- 4.1.2.3 Interview notes evidencing that the requirements set out in **4.1.2.2** above have been addressed shall be taken by the organisation and retained on the personnel file of the applicant.

The auditor shall select a number of personnel files to verify that interview notes are held on the personnel file and that the requirements have been met.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 2

4.1.3 Character and Other References

- 4.1.3.1 Screening procedures shall include direct reference to former employers, educational authorities, etc., with confirmation by them, in writing, of periods of employment contributing to a continuous record of the career or history of the person being screened for the whole of the screening period, on a month-to-month basis. The direct reference shall include at least one attempt, in writing, by the organisation to obtain the continuous record referred to in this requirement. Where no response is received to the request for information the requirements set out in **4.1.3.5** shall apply.

The auditor shall select a number of personnel files in order to confirm that the screening procedures have been applied and the requirements have been met. The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 1

4.1.3.2 Where initial references are taken by telephone the following procedures shall be used:

- a) The telephone number of the person called shall be confirmed independently.
- b) Information given on the telephone by a referee shall be noted at the time of making the telephone call and shall be signed and dated by the member of staff making the telephone call and retained on the individuals screening file (see **Annex A, Form 2** for a suggested format).
- c) A written request shall be forwarded to the referee within two working days of the telephone call being made seeking written confirmation of the information provided (see **Annex A, Form 3** for a suggested format).
- d) The screening process shall not be regarded as complete until written evidence is obtained.
- e) The progress sheet shall be used to monitor and record the action taken (see **Annex A, Form 4** for a suggested format).

The auditor shall ascertain the number of instances where references were taken by phone. The auditor shall inspect a selection of personnel files and confirm that the requirements set out in clause have been followed and are properly recorded.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 1

- 4.1.3.3 Only documents from third parties such as employers, colleges, Department of Social Protection, solicitors, accountants are acceptable for screening purposes.

Note. For the purposes of this document CVs or other personal documents are not acceptable as evidence of screening.

The auditor shall ascertain the number of instances where third party documents were provided for screening purposes and confirm that they are in accordance with the clause.
The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 1

- 4.1.3.4 Where records are not available, the period for which the record is not available shall be treated as a gap.

The auditor shall ascertain the number of records where a gap has been recorded. The auditor shall then ensure that clause 4.1.3.5 has been applied.

Non Compliance: Category 1

- 4.1.3.5 Where there are gaps in the career record which cannot be independently confirmed in accordance with the written verification procedures, the following procedure shall be followed:

- a) Written statements from personal referees shall be used, provided they had personal knowledge of the person being screened on a month-to-month basis during the period covered.
- b) The organisation shall be satisfied as to the creditability of the personal referee.
- c) The written statement shall as a minimum confirm that the applicant was where he/she purported to be and may, subject to the credibility of the referee, include a character reference.
- d) a progress sheet shall be used to monitor and record the action taken.

Note. For the purposes of this document personal referees shall not include family members, work colleagues or friends.

Where records have been identified under clause 4.1.3.4, the auditor shall inspect a selection of personnel files and confirm that the requirements set out in clause 4.1.3.5 have been followed and are properly recorded.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 1

4.1.4 Evidence of Qualifications/Awards

- 4.1.4.1 Prior to commencement of employment the organisation shall ensure that the applicant has any qualifications or awards necessary for the duties to which the applicant will be employed.

The auditor shall confirm that relevant qualifications/awards have been received and are properly recorded. Where possession of a PSA Licence is used as evidence of holding the required awards, the auditor shall confirm that the licence details were provided prior to employment commencing.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 1

4.1.5 Work Permits, Authorisations and Permissions

- 4.1.5.1 The organisation shall ensure that all necessary documentation for work visa applications and permissions/authority to work is fully completed before the individual is employed. This applies to renewal of such applications also.

The auditor shall ask the organisation if they currently employ any persons requiring permission to work in Ireland, or have had such employees since their last audit.

The auditor shall confirm that all necessary records associated with the required documentation for work visa applications and permissions to work are in place. Where none is declared, a signed written declaration must be provided.

Non Compliance: Category 2

- 4.1.5.2 The organisation shall maintain a register of all employees who have applied for and obtained permission or authorisation from the State to work in Ireland. The organisation shall review the validity of these permissions or authorisations at least every 6 months and shall keep a documented record of such reviews.

The auditor shall inspect the organisation's register of those employees who have applied for or hold permission to work in the State and confirm that the organisation is compliant with all requirements of clause 4.1.5. The auditor shall confirm that all permissions to work in the State are current.

Non Compliance: Category 2

- 4.1.5.3 The organisation shall ensure that the register at 4.1.5.2 is held on site at the address recorded on the Private Security Services Licence.

The register should be available on site and contain details of all employees requiring permission.

Non Compliance: Category 1

4.1.6 Maintenance and Retention of Records

- 4.1.6.1 The basic details of the employee, covering verifiable history within the industry, dates employed, positions held, disciplinary offences and a comment on suitability for employment in the security industry shall be retained for not less than five years from the date the employment ceases. This information shall be

verifiable in the form of readily retrievable records held at the organisations premises.

The auditor shall inspect a selection of personnel files and confirm that that they comply with the requirements contained in the clause.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 2

- 4.1.6.2 All records covered by 4.1.6.1 above shall be kept safe and secure against unauthorised access to, or alteration, disclosure or destruction of the data and against their accidental loss or destruction. Employers shall ensure that the records are retained for no longer than is necessary and in accordance with the recommendations of the Data Protection Commission.

The organisation shall provide the auditor with details of the storage arrangements for employee records.

Where records are accessed by computer this shall include details of firewalls and other security measures. The auditor shall be satisfied that such storage arrangements are in accordance with the requirements of the clause.

Non Compliance: Category 2

- 4.1.6.3 A list of all personnel currently employed both on a permanent and a probationary basis shall be maintained. In the case of those employed on a probationary basis, the dates on which probationary employment commenced and is to cease for each individual shall be recorded.

The auditor shall examine the list of current employees and ensure they are held and maintained in accordance with the clause.

Non Compliance: Category 2

4.1.7 Screening and Acquired Companies

- 4.1.7.1 Where it cannot be established by the records of an acquired organisation that screening to the required standard has already occurred, then this shall take place within a period not exceeding thirteen weeks from the date of acquisition.

Where applicable, the auditor shall confirm that screening has taken place in accordance with the clause.

Non Compliance: Category 1

4.2 Terms of Employment

- 4.2.1 All employees shall receive a clear, concise and unambiguous contract of employment and a staff handbook.

The auditor shall select a number of personnel files in order to confirm that that employees received a contract of employment and a staff handbook. A signed acknowledgement of receipt shall be on an employee's file.

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 1

- 4.2.2 In addition to any mandatory requirements, terms of employment shall include the following information:

- a) Job title.
- b) Effective start date.
- c) Probationary period.
- d) Pay and Allowances.
- e) Hours of work, days of work, shift frequency and shift variables.
- f) Holiday entitlement.
- g) Sick pay (conditions of payment) and pension entitlement.
- h) Industrial injury procedure.
- i) Location of place of work (employer's address).
- j) Equipment to be supplied.
- k) Disciplinary and grievance procedures.
- l) Terms of notice and termination.

- m) Copies of any Collective Agreement covering the employment.
- n) Appeals procedure.
- o) The Organisation's Health and Safety Statement.
- p) The Organisation's Equality policy.

The auditor shall confirm that terms of employment are in accordance with PSA requirements.

Non Compliance: Category 2

4.3 Code of Conduct

4.3.1 All employees shall be instructed that under the terms and conditions of employment they shall:

- a) Complete the required tasks promptly and diligently, unless there is due and sufficient cause not to.
- b) Ensure that all oral or written statements made by them, of whatever description, are true and accurate.
- c) Maintain carefully all documents and ensure that any alterations, disposal, or erasure of documents is carried out only with proper authorisation.
- d) Maintain confidentially on any matter relating to the employer or his clients either past or present.
- e) Ensure that any actions taken by them are such as not to bring discredit on the employer, the client or fellow employees.
- f) Immediately notify any conviction for a relevant criminal or motoring offence to the employer.
- g) Not allow unauthorised access to a client's premises.
- h) Ensure that they use employer's equipment or facilities only with authorisation.
- i) Continuously satisfy the requirements of PSA licensing.
- j) Hold on their person a PSA licence card at all times whilst on duty.

The auditor shall confirm that the organisations code of conduct is in accordance with PSA requirements.

Non Compliance: Category 2

4.3.2 The code of conduct shall be signed by all employees.

The auditor shall select a number of personnel files in order to confirm that the code of conduct has been signed by employees including any employees who have joined the organisation under the Transfer of Undertakings (Protection of Employment) Regulations (TUPE).

The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 2

4.3.3 Employers shall treat employees with courtesy and respect.

As per 4.3.1

4.4 Licence Card

4.4.1 The organisation shall ensure that all Enforcement Managers and Enforcement Guards have a valid PSA licence card.

From the 31st March 2023 until the 31st March 2024, Enforcement Managers and Enforcement Guards should hold a PSA Door Supervisor or a PSA Security Guarding licence.

Note: The PSA is currently developing a training course specific to enforcement guards. The new course will become the training requirement for enforcement guard licensing. The PSA expects to commence enforcement guard licensing for employees on the 31st March 2024.

The auditor shall confirm that the organisation complies with the requirements on licence cards contained in clause 4.4.1.

Non Compliance: Category 1

4.4.2 All employees shall be instructed on PSA requirements relating to the use of their licence card.

The organisation shall provide evidence that all employees have been instructed on the PSA requirements on licence cards

Non Compliance: Category 2

4.5 Uniform

4.5.1 The organisation shall provide each Enforcement Manager and each Enforcement Guard with an identical style of outer clothing, in this standard referred to as the uniform. The uniform shall remain the property of the organisation.

The organisation shall provide evidence that enforcement guard personnel have been provided with a uniform as required in clause 4.5.1

Non Compliance: Category 2

4.5.2 The uniform shall include colouring and lettering so to be readily distinguishable from the public and in a crowd. The uniform shall be green.

Lettering clearly indicating the word “ENFORCEMENT GUARD” shall be placed on the front left breast and the word “ENF. GUARD” on the back of the uniform and both should be clearly visible from a distance of 15 metres.

The word “ENFORCEMENT GUARD” shall be in uppercase letters and be not less than 1.5 centimetres high on the front left breast of the uniform. The word “ENF. GUARD shall be not less than 10 centimetres high on the back of the uniform. All lettering shall be permanently affixed to the uniform.

Note: All personnel wearing the uniform will be regarded as enforcement guards for PSA purposes.

The auditor shall inspect the organisation’s uniform and confirm that it meets the requirements specified in clause 4.5.2

Non Compliance: Category 3

4.5.3 The uniform shall be readily distinguishable from that of a member of the civil protection services.

The auditor shall confirm that the uniform is readily distinguishable from that of a member of the civil protection services

Non Compliance: Category 3

4.5.4 Each uniform shall contain a unique identity number on the front and back. The unique identity number shall be not less than 7 centimetres high and shall be clearly visible when the uniform is worn in normal working environments.

The auditor shall confirm that the uniform contains a unique identity number that meets the requirements of the clause

Non Compliance: Category 3

4.5.5 The uniform shall display insignia identifying the organisation providing the service and the wearer as an organisation employee. The organisation's insignia shall be clearly visible when the uniform is worn in normal working environments.

The auditor shall confirm that the organisation's insignia is clearly visible in accordance with the clause

Non Compliance: Category 3

4.5.6 All personnel wearing the uniform shall ensure that their facial features are clearly visible at all times. The wearing of head coverings are only acceptable for religious reasons.

The organisation shall provide a signed declaration confirming that personnel in uniform meet the requirements of the clause.

Non Compliance: Category 3

4.5.7 Subject to normal wear and tear the organisation shall provide for the renewal of uniforms.

The organisation shall advise the auditor on its procedures for the renewal of uniforms.

Non Compliance: Category 3

4.5.8 The cost of the uniform shall be borne by the organisation.

The organisation shall provide evidence that it complies with PSA requirements.

Non Compliance: Category 3

4.5.9 Where an employee leaves an organisation and the uniform is not returned to the organisation, the cost of the uniform may be deducted from any payment due to the employee.

The auditor shall review the organisation's arrangements for recouping the cost of uniforms where an employee leaves the organization.

Non Compliance: Category 3

4.5.10 A record of all uniforms not returned shall be retained by the organisation. The record shall contain the name of the employee, their PSA licence number and the unique identity number of the uniform.

The auditor shall review the organisation's record of uniforms not returned.

Non Compliance: Category 3

05—
Training



5. TRAINING

5.1 Training Policy and Responsibility

5.1.1 The organisation shall have a clearly defined, documented training policy, authorised at senior management level within the organisation. The policy shall cover theoretical and practical skills and meet any training requirements laid down by the PSA.

The auditor shall inspect the organisation's training policy document and verify that it has been authorised at senior management level within the organisation. The policy shall comply with the training requirements contained in clause 5.1.1 of PSA 91:2023.

Non Compliance: Category 1

5.1.2 The organisation shall appoint a member of the management team as training administrator.

The organisation shall advise the auditor of the name of the person appointed as the training administrator. The name together with any relevant qualifications shall be recorded in the audit report.

Non-Compliance: Category 3

5.1.3 The organisation shall ensure that all relevant staff meet the training requirements prescribed by the PSA.

The auditor shall inspect the training records and confirm that the organisation complies with PSA requirements

Non Compliance: Category 1

5.1.4 The training policy shall include a commitment to assess the effectiveness of all operational staff and to provide additional training where required.

The auditor shall verify that the training policy includes procedures to assess staff and provide additional training.

Non-Compliance: Category 2

5.2 Induction Training

- 5.2.1 Training shall include a detailed organisation-specific, induction session covering organisation structure, ethos, policies and employee roles and responsibilities for all newly recruited employees. This element of training shall be delivered before the employee commences operational duties. The training shall ensure that the employee understands and is able to act, at all times, professionally and within the bounds of the relevant legislation. Each employee shall acknowledge receipt of this training and associated documentation by signing a declaration. Such training shall be delivered by a competent member of staff and shall be recorded and this record shall be retained.

The auditor shall examine the training records of a selection of new employees and confirm that they have been certified as having received this training in accordance with PSA requirements. The auditor shall record the number and ratio of records examined.

Non Compliance: Category 2

5.3 Specialist Training

- 5.3.1 Employers shall ensure that employees required to carry out duties or use equipment of a specialist nature are certified as having received the appropriate training in the subject matter.

The auditor shall identify employees that are required to carry out duties or use equipment of a specialist nature and confirm that they have been certified as having received this training in accordance with PSA requirements. The auditor shall record the number and ratio of records examined, or 'none' where no specialist training is required.

Non Compliance: Category 2

- 5.3.2 Where risks are identified, in the course of carrying out a risk assessment, additional training, specific to these risks, shall be provided where training has not previously addressed the nature of the risk(s) involved.

The auditor shall examine the organisation's risk register and identify if any risks outlined in the clause were identified and record details of training provided. Where risks have been identified the auditor shall seek training details to address such risks.

Non Compliance: Category 2

5.4 Refresher Training

- 5.4.1 Procedures shall exist to assess the effectiveness of all employees, and where required refresher training shall be carried out.

The auditor shall inspect the organisation's procedures in place to identify and carry out refresher training. The auditor shall identify employees that require refresher training and have received this training in accordance with PSA requirements.

Non Compliance: Category 2

5.5 Supervisory and Management Training

- 5.5.1 Subject to PSA requirements and any associated guidelines, the organisation shall ensure that all operational supervisory and management staff receive documented training in consideration of their position and responsibilities.

The auditor shall verify that all operational supervisory and management staff have received training in accordance with PSA requirements. The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 2

5.6 Training Records

5.6.1 The training administrator shall ensure that proper training records are maintained.

The auditor shall select a number of training records in order to confirm that PSA requirements have been met. The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 2

5.6.2 Individual training records relating to training provided by the organisation shall indicate the date, training organisation, details of certification and subject(s) covered. These training records shall be signed by the employee and countersigned by the training administrator and retained as part of the employee's record.

The auditor shall select a number of training records in order to confirm that PSA requirements have been met. The auditor shall record their findings together with the number and ratio of records selected, in the report.

Non Compliance: Category 2

5.6.3 Verification of all training shall be available for inspection at the address recorded on the Private Security Services Licence.

The auditor shall have access to the training records to ensure all requirements are being met.

Non Compliance: Category 2

5.6.4 All refresher training undertaken by employees shall be recorded and the record held and retained on the employee's personnel file by the employer.

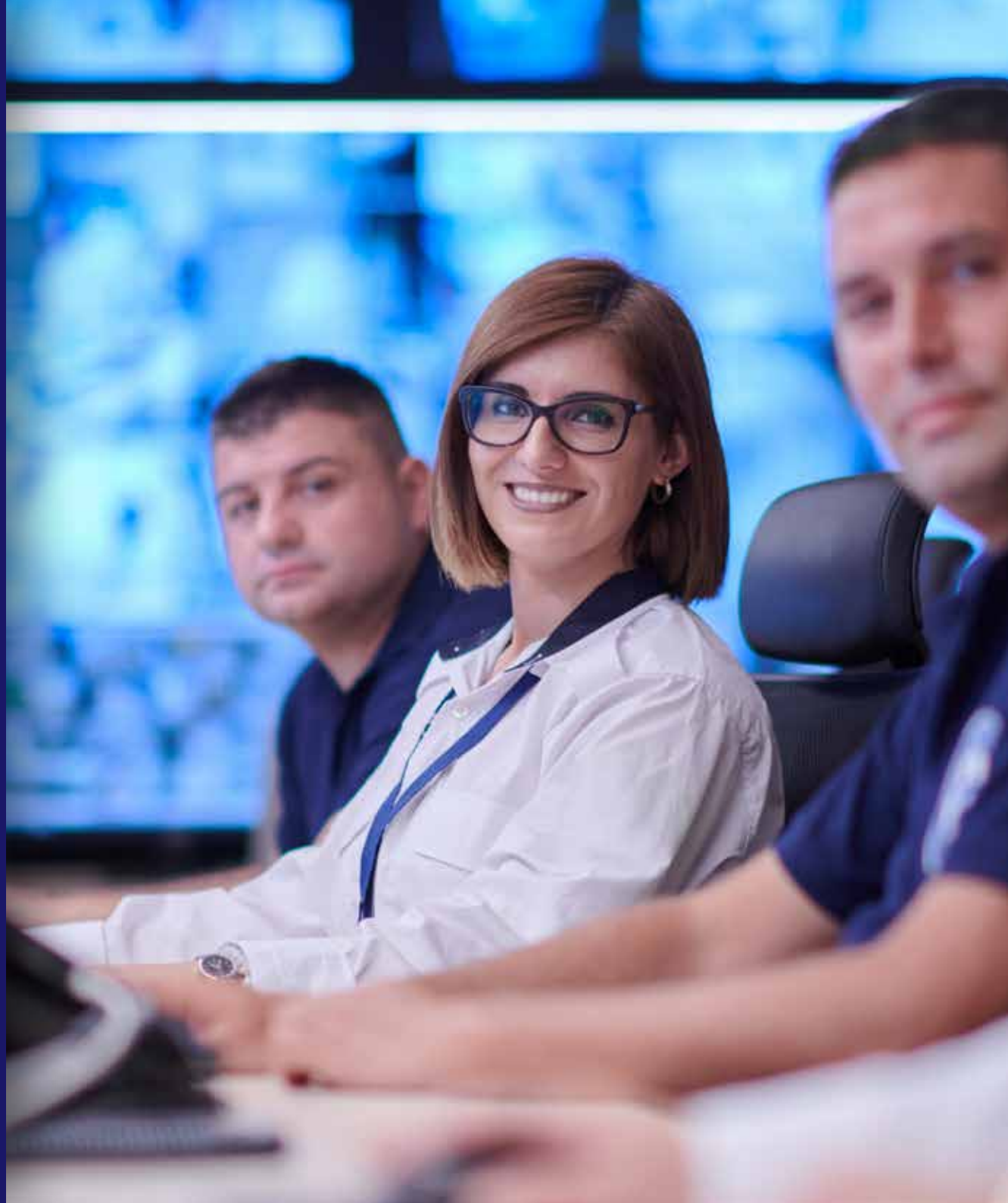
As per 5.5.1

5.6.5 Records shall indicate where further training is required.

A schedule of planned training shall be completed.

Non Compliance: Category 2

06—
Operations



6. OPERATIONS

6.1 Risk Assessments

- 6.1.1 The organisation shall carry out a detailed and documented risk assessment survey on each site documenting the potential risks including security risks, risk to persons on the site, risks to the public and risks to the health and safety of each employee on duty at the site.

The auditor shall inspect the organisation's risk assessment surveys and confirm that they have been undertaken for each site. Auditors may choose a random selection of surveys where the volume dictates.

In selecting surveys, the auditor should in the first instance, check the surveys for those contracts which have been inspected under clause 3.5.2

Non Compliance: Category 1

- 6.1.2 The risk assessment shall be in accordance with the risk assessment guidelines contained in **Annex B** to this document.

The auditor shall confirm that the risk assessments are in compliance with the risk assessment guidelines contained in Annex B

Non Compliance: Category 1

- 6.1.3 A Security Management Plan shall be prepared for each site and shall be available to the client and authorised officials. Where applicable, the plan shall include but shall not be limited to the following:

- a) the name and contact details (email and mobile phone number) of the representative of the organisation responsible for the implementation of the plan;
- b) the risk assessment and risk control plan (always applicable);
- c) Numbers of staff and general designation, where defined (always applicable) e.g.
 - Command and Control System team,
 - Supervisors,
 - Enforcement Guards identified by role, for example those responsible for removal of persons, seizure of goods, controlling access and perimeter;

- d) Location and time of pre-operation briefing session (always applicable);
- e) Crowd management including policy and procedures on searches and removal of persons;
- f) Major incident planning;
- g) Identification of staff (always applicable);
- h) Communications equipment (always applicable);
- i) Body Cameras to be worn during the provision of the security service and shall meet all data protection provisions;
- j) Traffic management plan as agreed with local Garda Superintendent;
- k) Health and safety of staff (always applicable);
- l) Personal risk assessment of staff (always applicable);
- m) Site plan (always applicable);
- n) Details of any subcontractors on site and their role (e.g., locksmiths, alarm technicians etc.);
- o) Inclusion of subcontractor's method statement/risk assessment for the specialist tasks they must carry out;
- p) Details of any statutory bodies on site and their functions.

The auditor shall inspect the organisation's security management plan and confirm that they have been prepared for each site and that they satisfy the requirements of 6.1.3.

Auditors may choose a random selection of surveys where the volume dictates.

Non Compliance: Category 1

- 6.1.4 All Enforcement Guards shall wear body cameras. The cameras shall be issued to each Enforcement Guard and will only be in use during the periods of operation as set out by the Security Management Plan.

The organisation shall provide evidence that all enforcement guards are issued with and wear body cameras during the provision of enforcement guard security services.

Non Compliance: Category 1

6.1.5 The use of body cameras shall be subject to a Data Protection Impact Assessment (DPIA) and the Data Controller of the organisation is responsible for ensuring that the use of such cameras meet all data protection provisions.

The auditor shall verify that the organisation has completed a Data Protection Impact Assessment (DPIA) in respect of the use of body cameras and data protection requirements.

Non Compliance: Category 1.

6.1.6 The organisation shall have a Body Camera User Policy in place.

The auditor shall verify that the organisation has a Body Camera User Policy in place.

Non Compliance: Category 1.

6.1.7 When the body cameras are in use the Enforcement Guard shall indicate to all persons that recording is active and operational via indicator light, switch or slide activation, visible badge, a combination of these indicators or otherwise so that all persons being recorded are aware that the body camera is in record mode.

The auditor shall verify that the organisation's Body Camera User Policy includes the requirement that Enforcement Guards advise persons when recording is activated.

Non Compliance: Category

6.1.8 When the body cameras are not in use, they shall be stored in a safe and secure facility with access restricted to designated officers of the organisation as identified in the DPIA.

The auditor shall inspect the storage facility and confirm that it meets the requirements of 6.1.8

Non Compliance: Category 1

6.1.9 All persons required to use body cameras shall have received appropriate and relevant training in the use of the equipment prior to any operation.

The auditor shall identify employees that require body camera training and verify that they have received this training in accordance with PSA requirements. The details shall be noted on the report.

Non Compliance: Category 1.

6.1.10 The number of Enforcement Guards on duty shall depend on the risk assessment and Security Management Plan and shall be determined in consultation with the client.

The auditor shall confirm the number of Enforcement Guards on duty has been determined in accordance with the risk assessment and security management plan in consultation with the client.

Non Conformance: Category 1

6.1.11 Notwithstanding the requirements of sub-clause **6.1.10** the organisation shall as a minimum provide the following:

- a) at least two Enforcement Guards for each access and egress point to be secured;
- b) three Enforcement Guards for each team that is required to remove persons from a site;
- c) two Enforcement Guards for each team that is required to remove goods or property.

The auditor shall verify that the requirements of 6.1.11 have been satisfied at each site audited.

Non Conformance: Category 1

6.1.12 All Enforcement Guards shall attend a pre-operation briefing session held at a site other than the project site, the content of which shall relate directly to the service being provided, the duration and subject matter of the briefing session depending upon the complexity of the site and operation.

The auditor shall confirm that all Enforcement Guard personnel have been briefed in accordance with clause 6.1.12 and 6.1.14

Non Conformance: Category 1

- 6.1.13 In addition to the pre-operation briefing session each Enforcement Guard and subcontractors shall receive written assignment instructions on what their duties and responsibilities are.

The auditor shall confirm that all Enforcement Guards and subcontractors received written assignment instructions in accordance with 6.1.13

Non Conformance: Category 1

- 6.1.14 Verification of the pre-operation briefing session shall take the form of an attendance register with the names of attendees in block capitals. The register shall be signed by the attendees including subcontractors, countersigned and dated by the organisation's management.

The auditor shall inspect the Pre-operation briefing session register and confirm that it satisfies meets PSA requirements.

Non Conformance: Category 1

- 6.1.15 A copy of the countersigned attendance register shall be attached to the Security Management Plan.

The auditor shall confirm that the pre-operation briefing session register is attached to the Security Management Plan in accordance with PSA requirements

Non Conformance: Category 1

6.2 Times and Hours

- 6.2.1 Enforcement Guards should be respectful of the religion and culture of others at all times. Consideration should be given to the appropriateness of undertaking enforcement on any day of religious or cultural observance or during any major religious or cultural festival.

The auditor shall confirm that Enforcement Guard services take place in accordance with PSA requirements.

Non Conformance: Category 2

- 6.2.2 Enforcement action in residential settings should only be carried out between the hours of 6.00am and 9.00pm, unless otherwise authorised by a court and in line with relevant legislation. There are no time restrictions on enforcement action in commercial or business premises.

The auditor shall confirm that Enforcement Guard services take place in accordance with PSA requirements

Non Conformance: Category 2

6.3 Mode of entry

- 6.3.1 Enforcement Guards shall not seek to gain entry to premises under false pretences.
- 6.3.2 Enforcement Guards shall only enter premises as part of the enforcement process.
- 6.3.3 Enforcement Guards shall only use a door or other usual means of entry.
- 6.3.4 The power to enter a premises by force shall only be used when it is reasonably required and only after the Enforcement Manager has authorised the use of said power.

The auditor shall confirm that the mode of entry used meet PSA requirements

Non Conformance: Category 2

6.4 Goods

- 6.4.1 Enforcement Guards shall only seize goods or other property in accordance with the terms of the court order.

The auditor shall confirm that goods or property seized are in accordance with legislation.

Non Conformance: Category 2

- 6.4.2 Enforcement Guards shall ensure that goods are handled with due care whilst in their possession. The organisation shall have insurance in place for goods in transit.

The auditor shall confirm that the transport of goods meet PSA requirements.

Non Conformance: Category 2

- 6.4.3 Enforcement Guards shall not remove anything clearly identifiable as an item belonging to, or for the exclusive use of a person under the age of 18 or items clearly identifiable as required for the care and treatment of the disabled, elderly and seriously ill.

The auditor shall confirm that the seizure of goods meet PSA requirements.

Non Conformance: Category 2

- 6.4.4 A detailed list of all goods removed shall be recorded.

The auditor shall inspect the list of goods removed and confirm that it meets PSA requirements.

Non Conformance: Category 2

6.5 Vulnerable situations

- 6.5.1 The organisation and their client have a responsibility to ensure that guidelines are in place on how to proceed where persons have been identified as vulnerable as defined at 2.25 of the definitions in this standard. The use of discretion is essential and the organisation has a duty to contact the client to report the circumstances in situations where there is evidence of possible concern.

The auditor shall inspect the organisation's guidelines in respect of vulnerable persons and confirm that the guidelines meet PSA requirements.

Non Conformance: Category 1

- 6.5.2 The organisation must withdraw from domestic premises if the only person present is, or appears to be, under the age of 18 or is deemed to be vulnerable by the Enforcement Guard.

The auditor shall confirm that Enforcement Guard services are provided in accordance with PSA requirements

Non Conformance: Category 1

6.6 Enforcement Manager

- 6.6.1 The organisation shall appoint a suitably qualified person as Enforcement Manager who shall be responsible for the management of all security services provided by the organisation. The person appointed should hold a managerial position within the organisation.

The auditor shall confirm that the organisation has appointed an Enforcement Manager in accordance with PSA requirements.

Non Conformance: Category 1

- 6.6.2 The Enforcement Manager shall be responsible for ensuring compliance with all PSA legislation, regulations and requirements during the provision of the security service.

The auditor shall confirm that the organisation satisfies PSA requirements.

Non Conformance: Category 1

- 6.6.3 The Enforcement Manager shall be on site at all times when a security service is being provided.

The auditor shall confirm that the organisation satisfies PSA requirements.

Non Conformance: Category 1

- 6.6.4 The Enforcement Manager shall be in communication with the Command and Control System at all times

The auditor shall confirm that the organisation satisfies PSA requirements.

Non Conformance: Category 1

- 6.6.5 All Enforcement Guards shall report to the Enforcement Manager and shall be responsible for all security tasks assigned to them by the Enforcement Manager.

The auditor shall confirm that the organisation satisfies PSA requirements.

Non Conformance: Category 1

- 6.6.6 The appointment of a licensed Enforcement Guard to act as an Enforcement Manager is allowable where the Enforcement Manager is not available.

The auditor shall confirm that the organisation satisfies PSA requirements.

Non Conformance: Category 1

6.7 Command and Control Systems

6.7.1 Facilities shall be in place to provide for the following:

- a) The provision, or procurement, of assistance or advice in routine and emergency situations.
- b) The recording of all appropriate routine and emergency matters to enable management to deal quickly and efficiently with the organisation's contractual responsibilities.

The auditor shall inspect the organisation's command and control facilities and confirm that they meet PSA requirements of Clause 6.7.1

Non Conformance: Category 1.

6.7.2 The organisation shall have a command and control system that is:

- a) Located at the organisation's own fixed location, or
- b) A contracted service with a PSA licensed Monitoring Centre.

The auditor shall confirm the type of command and control system provided by the organisation.

Non Conformance: Category 1

6.7.3 The following minimum provisions shall apply for all command and control systems.

- a) Manning of the operations command and control system shall be consistent with the anticipated workload and the nature of the work.
- b) Appropriate first aid and firefighting equipment shall be provided within the command and control system.
- c) Management shall review and update command and control system information and procedures at least once every 12 months.
- d) Management shall produce a command and control system manual covering all foreseeable contingencies for the guidance of controllers.
- e) The manual shall contain instructions for controllers to enable them to deal effectively with all foreseeable contingencies and shall clearly indicate the stage at which any incident requires the controller to pass on information to a more senior person.

- f) A copy of the manual shall be readily available within the command and control system at all times.
- g) Comprehensive instructions outlining action to be taken on receipt of verbal incident reports shall be provided.
- h) There shall be clearly defined procedures for management follow-up in relation to incidents, and also in relation to responses and supports available to staff in the event of an incident.
- i) All command and control staff shall be required to partake in practice drills for responses to emergency situations which might endanger the health and safety of staff. Such drills shall take place at least once every 12 months and the outcome(s) of the drills shall be documented and recorded.

The auditor shall confirm that the organisation's command and control system meets PSA requirements

Non Conformance: Category 1

6.7.4 The following additional provisions shall apply where the organisation operates its own dedicated fixed location command and control facility:

- a) Staff manning the command and control facility shall hold a PSA Enforcement Guard or Security Guard (Guarding) or Security Guard (Monitoring Centre) licence.
- b) The equipment, furnishings and layout of the command and control system shall be consistent with the efficient operation of the system.
- c) There shall be access to kitchen and bathroom facilities.
- d) Heating, lighting and ventilation shall be provided to ensure a reasonable working environment.
- e) The command and control system shall be a restricted area open only to those authorised to enter. A means of secure physical restriction shall exist to prevent access by unauthorised persons to the command and control system.

The auditor shall confirm where the organisation operates its own dedicated fixed location company and control facility it meets PSA requirements.

Non Conformance: Category 1

6.7.5 Where a contracted facility is used the organisation shall ensure by initial inspection and documented report that the facility satisfies the requirements of this section and that adequate documented and physical procedures are in place to ensure security of all clients information and access media.

The contract shall include a provision for ongoing periodic inspection and reporting on compliance by the contracted facility to these requirements.

Where contracted command and control facilities are used, the auditor shall inspect the organisation's report on the suitability of the facilities available.

Such report should include details of the physical security of the premises and the procedures in place to protect clients' details.

The organisation should undertake a review of the facility once each year to ensure that it complies with PSA requirements.

The name of the contractor operating the facility, their address and where applicable, their PSA licence number should be recorded in the audit report.

Non Conformance: Category 1

6.7.6 Authorised Officials may access the command and control system for the purpose of verifying compliance with the requirements of PSA licensing.

The auditor shall confirm that access to the command and control system for compliance verification purposes meets PSA requirements.

Non Conformance: Category 1

6.8 Incident Reporting

6.8.1 All operational staff shall be made aware in writing of the identity of the Enforcement Manager and any other member of staff to whom they report and the method of reporting of incidents or problems to the organisation's management, in both urgent and non-urgent cases.

The auditor shall confirm operational staff were made aware, in writing, of the identity of the Enforcement Manager (in writing) and staff members to who they report, including the method of reporting of incidents or problems in accordance with PSA requirements.

Non Conformance: Category 1

6.8.2 All incidents shall be handled by the Enforcement Manager in the first instance and recorded in the Incident Report. The Incident Report shall contain as a minimum the following details:

- a) Date, time and place of the incident.
- b) Date and time of reporting and by whom reported.
- c) Nature of the incident.
- d) Full description of events leading up to the incident, the incident itself and events following the incident.
- e) Details and rationale behind the use of any force during the incident.
- f) Action taken, including onward reporting.
- g) Further action to be taken.
- h) Where possible, names and addresses of all relevant persons present.

The auditor shall confirm that incident reports meet PSA requirements.

Non Conformance: Category 1

6.8.3 Facilities shall be in place to provide for the following:

- a) The recording of all appropriate routine and emergency matters to enable management to deal quickly and efficiently with the organisation's contractual responsibilities.
- b) There shall be clearly defined procedures for management follow-up in relation to incidents, and also in relation to responses and supports available to staff in the event of an incident.

The auditor shall inspect the organisation's facilities in place for the recording of all appropriate routine and emergency matters and the procedures in place for management follow-up in relation to incidents, including responses and supports available to staff in the event of an incident.

Non Conformance: Category 1

6.8.4 There shall be in place an organisation escalation policy for client liaison.

The auditor shall inspect the organisation's escalation policy for client liaison.

Non Conformance: Category 1

6.8.5 The Organisation shall maintain a record of all reported incidents for a minimum of three years or for such longer periods where required by law.

Entries shall be numbered sequentially and serially and shall include time, date, record of notification of the client and the name of the Enforcement Manager completing the record.

The auditor shall inspect the organisation's records of reported incidents to confirm it is in accordance with PSA requirements.

Non Conformance: Category 1

6.9 Threats and Violence

6.9.1 The organisation shall, as part of its risk assessment, assess the risks for violence that employees can reasonably be expected to be exposed to and shall outline and implement risk mitigating measures to eliminate or significantly diminish any identified risks (see **6.1**).

The auditor shall inspect the organisation's risk assessment and confirm that it meets PSA requirements.

Non Conformance: Category 1

6.9.2 Risk mitigating measures shall include special training and safety routines in place where the risk assessment has shown that there is a significant likelihood and severity of consequence of violence.

Personal Protective Equipment (PPE) shall be provided where it has been identified as a risk mitigation measure.

The auditor shall confirm that where the risk mitigating measures include special training and safety routines that these have taken place.

Non Conformance: Category 1

6.9.3 Safety routines shall be kept continuously updated and shall be made known to all employees, particularly where duties or locations are involved that have been identified in the risk assessment as carrying a higher than normal risk of physical violence occurring. The employer shall ensure that these employees shall be educated, trained and informed in relation to the identified risks.

The auditor shall confirm that safety routines are continuously updated where necessary and that employees are informed, trained and educated in accordance with PSA requirements.

Non Conformance: Category 1

6.9.4 Tasks involving a high risk of violence shall be identified in the risk assessment and meet the requirements of 6.1.5.

The auditor shall inspect the organisation's risk assessment and confirm that tasks involving a high risk of violence meet PSA requirements under clause 6.1.5

Non Conformance: Category 1

6.9.5 Incidents involving violence shall be recorded and investigated fully by the organisation and notified to An Garda Síochána. Any remedial course of action recommended as a result of the investigation shall be acted upon by the organisation within reasonable timeframes.

The auditor shall inspect the organisation's risk assessment and confirm that it meets PSA requirements.

Non Conformance: Category 1

- 6.9.6 The organisation shall ensure that appropriate physical and psychological support is available, on request, to any employee who has been subjected to violence as a result of carrying out his/her duties.

The organisation shall provide details of support procedures in place for employees who have been subjected to violence in the course of carrying out their duties.

Non Conformance: Category 1

6.10 Operations Records

- 6.10.1 Records shall be maintained for a period not less than three years for each site, which shall include following information;
- a) The service provided and the name of the client(s);
 - b) Location where the service was provided;
 - c) Details of the court order including Court reference;
 - d) Name and PSA Licence Number of the Enforcement Manager;
 - e) Name, PSA licence number, uniform unique identity number, identification number or works number of each person employed as an Enforcement Guard;
 - f) Details of all calls made to the command and control system;
 - g) CCTV/Body Camera footage.

Upon expiration of the required retention period the organisation shall dispose of the relevant records in a secure and confidential manner.

Note: National legislative requirements may entail retention of records for longer periods of time.

The auditor shall inspect the organisation's operations records to confirm that they meet PSA requirements.

Non Conformance: Category 1

- 6.10.2 A facility shall exist for the checking and reviewing of incident reports and reporting procedures periodically by senior management of the organisation. A record of such checks and reviews shall be maintained for a period of 5 years.

The auditor shall inspect the organisation's facilities for the checking and reviewing of incident reports by senior management. The auditor shall inspect the organisation's record of these checks and reviews.

Non Conformance: Category 1

6.11 Assignment Instructions

- 6.11.1 In consultation with the client, the organisation shall formulate assignment instructions, which will encompass full operational instructions for the effective execution of the security service, detailing emergency procedures, lines of communication and accountability.

The auditor shall inspect the organisation's assignment instructions to confirm that they meet PSA requirements.

Non Conformance: Category 1

- 6.11.2 The assignment instructions shall be agreed and endorsed by the client. Any alteration to the instructions shall be endorsed by the organisation and the client as soon as practicable. Where the client chooses not to endorse assignment instructions the organisation shall maintain evidence on file of e-mailing or postage (registered) of delivery to the client and any subsequent correspondence.

The auditor shall inspect the organisation's assignment instructions to confirm that they meet PSA requirements.

Non Conformance: Category 1

6.11.3 The assignment instructions shall be available in the Security Management Plan and a copy shall be available to the client.

The auditor shall confirm that the assignment instructions are available in the Security Management Plan and that a copy is available to the client in accordance with PSA requirements.

Non Conformance: Category 1

6.11.4 Assignment instructions shall include:

- (a) Details of the full extent of the services to be provided;
- (b) The procedure for contacting the organisation's command and control system;
- (c) Details of the service to be provided including:-
 - i. the number of personnel involved in the assignment and their responsibilities,
 - ii. the maximum hours allowed for which the service is to be provided shall be 48 hours and handover instructions at start and end of service,
 - iii. where security is required after the 48 hour period it shall be provided by a licensee in the Security Guarding sector,
 - iv. facilities, vehicles or equipment provided,
 - v. safety statement,
 - vi. welfare facilities for staff;
- (d) A site plan of the location;
- (e) Any relevant extracts from the Security Management Plan.

The auditor shall inspect the organisation's assignment instructions and shall confirm that they comply with PSA requirements.

Non Conformance: Category 1

6.11.5 Each Enforcement Guard shall receive individual assignment instructions which shall include the following;

- a) Full details of their roles and responsibilities;
- b) Name and contact details of their supervisor/manager;
- c) Name and contact details of the Enforcement Manager if not included

- under (b);
- d) Location and time of pre-operation briefing session;
 - e) Start time and duration of operation;
 - f) Address of site and site plan;
 - g) Procedures for reporting incidents and responding to incidents;
 - h) Escalation procedures in the event that the procedure at (g) cannot be activated.

The auditor shall inspect a sample of individual assignment instructions issued to Enforcement Guards and shall confirm that they comply with PSA requirements.

Non Conformance: Category 1

6.12 Security of Information and Access Media

- 6.12.1 Clear and unambiguous routines shall be established for staff to deal securely with any confidential information to which they have access in the course of operations.

The auditor shall inspect the organisation's routines for staff dealing with confidential information and confirm that they meet PSA requirements.

Non Conformance: Category 1

- 6.12.2 Organisations shall keep confidential any knowledge of their clients' business or operations acquired through the provision of services. In particular, structures and procedures shall be put in place and implemented to ensure that any details relating to the client's security equipment, procedures and practices must be subject to the appropriate level of access within the organisation's business.

The auditor shall confirm that the organisation complies with PSA requirements.

Non Conformance: Category 1

- 6.12.3 Any details relating to the client's business, premises, residence, assets, procedures or any other aspect of knowledge of the client gained by the organisation and employees, the disclosure of which can be reasonably construed as compromising the business or security of the client, shall not be

disclosed or made known in any way to a third party or third parties, except with the express written permission of the client.

Where written permission is granted, the organisation shall retain this on file and shall produce this if requested by an appropriate authority.

The auditor shall confirm that the organisation complies with PSA requirements.

Non Conformance: Category 1

- 6.12.4 All confidential information held in electronic format by the organisation shall be backed up at least once a week. Back-up records shall be held in such a manner that a threat or threats to the integrity of one set of records will not pose a threat to the other set.

The auditor shall inspect the backup records and confirm backup and storage is in accordance with PSA requirements.

Non Conformance: Category 1

- 6.12.5 It shall be a condition of any contract that requires the organisation to hold keys that such keys shall only be surrendered to an authorised representative of the client upon receipt of a written request to do so.

The auditor shall confirm that the organisation's procedures in respect of the holding and surrender of client keys are in accordance with PSA requirements.

Non Conformance: Category 1

- 6.12.6 Retention and storage of data relating to CCTV/Body Camera footage taken at the site shall be in line with Data Protection legislation.

All notices, correspondence and documentation issued by the organisation must be clear and in agreement with the client and should comply with relevant legislation.

The auditor shall confirm that the organisation's procedures in respect of the retention and storage of data relating to CCTV/Body Camera footage is in line with Data Protection legislation and in accordance with PSA requirements.

Non Conformance: Category 1

- 6.12.7 The organisation should provide a report to the client on any un-executed orders/warrants.

The auditor shall confirm that the organisation has provided a report to clients where there are any un-executed orders/warrants in accordance with PSA requirements.

Non Conformance: Category 1

6.13 Vehicles and Equipment

- 6.13.1 All operational vehicles used by the organisation shall, unless exempted by the risk assessment, clearly display the organisation's name and PSA licence number.

The auditor shall inspect a sample of the organisation's vehicle(s) and confirm that they comply with PSA requirements.

Non Conformance: Category 3

- 6.13.2 Vehicles shall carry a two-way communication capability, a dry powder fire extinguisher and a first aid kit.

The auditor shall confirm that vehicles carry a two-way communication capability, a dry powder fire extinguisher and a first aid kit.

Non Conformance: Category 2

- 6.13.3 Organisations shall ensure that driving licences of staff involved in driving operational vehicles are valid for the duration of each such employee's period of employment. Copies of all driving licences shall be held on the employee's file.

The auditor shall request details of all staff involved in the driving of vehicles and inspect the employee's files to ensure that they comply with PSA requirements.

Non Conformance: Category 2

- 6.13.4 Drivers shall complete a history form, to be verified and maintained by the organisation, with all accidents and convictions recorded on this form.

The auditor shall inspect driver's history forms and confirm that they have been verified by the organisation.

Non Conformance: Category 2

6.13.5 All marked vehicles shall be readily distinguishable from those of any elements of the civil protection or emergency services.

The auditor shall confirm that marked vehicles are readily distinguishable from those of the civil protection or emergency services.

Non Conformance: Category 3

6.13.6 The organisation shall provide all drivers with clearly defined instructions on their role including details of the movement of the vehicle during operations, actions to be taken on foot of incidents, accident procedures, carrying of passengers, etc.

The auditor shall confirm that the organisation has provided all drivers with clearly defined instructions in accordance with PSA requirements.

Non Conformance: Category 3

6.13.7 All vehicles and equipment used in connection with the provision of services shall be in working order and be regularly maintained and serviced.

The auditor shall inspect the maintenance and service documentation of the organisation's vehicles and equipment and confirm that maintenance and service is in accordance with manufacturer's recommendations.

Non Compliance: Category 3

6.13.8 All employees shall sign for all equipment issued and give an undertaking to return any equipment issued immediately on request.

The auditor shall inspect the organisation's procedures for the issue and return of equipment.

Non Compliance: Category 3

07—
Compliance
with PSA
Licensing



7. COMPLIANCE WITH PSA LICENSING

7.1 Compliance with Standards

7.1.1 Organisations shall maintain compliance with this standard during the term of their 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 91:2023 which come to their attention in the audit report.

Non Compliance: Category 1

7.1.2 Organisations shall be subject to an audit by a PSA appointed auditor 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 a period not exceeding 12 months has passed since the last audit. If a period exceeding 12 months has passed the reasons for the extended period shall be recorded. Where the extended period was due to circumstances under the organisation's control it shall be recorded as a non compliance.

Non Compliance: Category 1

7.1.3 An audit report shall be completed by the auditor for each audit undertaken and the organisation shall agree to the auditor providing a copy of the report to the PSA.

The auditor shall confirm that the organisation has agreed that a copy of the audit report shall be provided to the PSA.

Non Compliance: Category 1

7.1.4 Organisations shall give their permission to the auditor to provide the PSA with information in accordance with provisions 7.1.5 and 7.1.6

The auditor shall confirm that the organisation has agreed that a copy of the audit report shall be provided to the PSA.

Non Compliance: Category 1

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

Non Compliance: Category 1

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

Non Compliance: Category 1

7.2 PSA Licensing Requirements

7.2.1 The organisation shall ensure that an inspector appointed by the PSA, may at any time, enter any place where a security service is being provided and provide any information requested by an inspector in the course of any inspection or investigation.

Non Compliance: Category 1

7.2.2 Organisations shall be familiar with all legislation relevant to the provision of their business.

The auditor shall seek a statement signed by the principal of the organisation confirming that it is familiar will all legislation relevant to the provision of their business.

Non Compliance: Category 2

7.2.3 During the term of the licence organisations shall comply with all relevant and current legislation and specifically the following:

- a) The Private Security Services Acts and Regulations.
- b) Organisation of Working Time Acts.
- c) Taxation and Social Welfare Acts.
- d) Payment of Wages Acts.
- e) Immigration Acts.
- f) Health and Safety at Work Regulations.
- g) Companies Act 2014 (where appropriate).

- h) Data Protection Acts.
- i) Irish Human Rights and Equality Commission Act 2014.

The auditor shall confirm that the organisation complies with PSA requirements

Non Compliance: Category 2

7.2.4 The organisation shall within 7 days notify the PSA in writing if any of the following occur:

- a) Change of name of the licence holder.
- b) In the case of a body corporate, change in directors.
- c) In the case of a partnership, change in partners.
- d) Change of ownership of the organisation. In the case of a body corporate, this includes a change in any shareholding above 5%.
- e) Commencement and cessation dates of employment of all enforcement guards.
- f) Change of address from which the security service is being provided.
- g) Change of registered address if this is different from address at f) above.
- h) Change in the legal status of the licence holder.
- i) Any conviction against the licence holder whether in relation to the business of the licence holder or other matter. In the case of a body corporate, this includes any convictions against a director. In the case of a partnership, this includes any convictions against a partner.

The Auditor shall confirm that the organisation complies with PSA requirements.

Non Compliance: Category 2

ANNEX A Screening Forms

Form 1

FORM OF AUTHORITY

I, _____, (BLOCK CAPITALS) hereby
authorise _____

to supply full details of my employment record with the organisation or business in furtherance of
my current application for employment in event security.

1. Address at time of employment with the organisation _____

2. PPS No. _____

Signed: _____ Date: ____/____/____

RECORD OF ORAL ENQUIRY

Name of Applicant: _____

PPS No: _____

Name of Previous Employer: _____

Telephone No: _____

Person Contacted: _____

Dates Employed: - As stated by employee: From _____ To _____

- Confirmed by employer: From _____ To _____

- Would re-employ? _____

- Reasons for not re-employing*: _____

Reasons why applicant would not be suitable to work in security:

Signed: _____ Date: ___/___/___
(Person making enquiry)

Signed: _____ Date: ___/___/___
(Manager)

* Where response indicates that applicant is not suitable for proposed employment bring to immediate attention of Manager responsible for screening/recruitment.

Form 3

REQUEST FOR WRITTEN CONFIRMATION OF INFORMATION PROVIDED ORALLY

RE. Name of Applicant: _____

PPS No: _____

We refer to our conversation with you on the _____ regarding an application for employment in the Enforcement Guard sector of the security industry made by the above named applicant.

Details of the information which you provided to us orally are enclosed and we would be obliged if you would kindly confirm that these details fairly reflect the information supplied.

Our business is licensed by the Private Security Authority and is obliged by the Authority's regulations to obtain written confirmation of all references we receive in connection with applications for employment.

A copy of a Form of Authority signed by the applicant is enclosed and also a stamped addressed envelope for your reply.

Yours faithfully

Human Resources Manager

SCREENING PROGRESS REPORT*

Name of Applicant: _____

PPS No: _____

1. Employments contacted

	Date	Employers Name	Date Letter Sent	Initials	Date of Reply	Initials
1						
2						
3						
4						
5						

2. Screening reviewed

Date of review: __/__/__ Person Reviewing: _____

Action: _____ Initials: _____

3. Offer of Employment

Signed: _____ Date: __/__/__
(HR Manager or Principal of the organisation)

4. Employment refused

Signed: _____ Date __/__/__
(HR Manager or Principal of the organisation)

* This form is to be retained on the individual's file for any subsequent inspection.

ANNEX B Risk Assessment Guidelines

1. Scope

The purpose of these guidelines is to outline the process to be applied by Private Security Authority Licensed Contractors when undertaking Risk Assessments as required by Section 6.1 of the PSA Requirements Document “*PSA Licensing Requirements – Enforcement Guard*”.

2. Introduction

Risk assessment and management underlies the duties of PSA Licensed Contractors under the provisions of the PSA Requirements Document “*PSA Licensing Requirements – Enforcement Guard*”. Under this document a contractor must identify and assess the risks and select the appropriate control measures to eliminate or reduce those risks so far as is reasonably practicable pertaining to the provision of the security service. A contractor should consider the likelihood, consequences and ways of eliminating or reducing hazards or risks in determining what is reasonably practicable.

This document outlines the processes which should be undertaken along with some of the factors that should be considered by contractors when identifying risks, assessing risks and eliminating or controlling those risks. All elements of the process undertaken in accordance with these guidelines must be documented and available for inspection by the PSA and PSA appointed auditors.

The Requirements Document specifies that a risk assessment shall be undertaken for each site. The extent and level of documentation of risk identification, risk assessment and risk control measures will depend on the circumstances at the time and the likely level of exposure to any risk.

The risk assessment shall be undertaken by a person with competence in security risk identification and in risk assessment and who has the ability to assess all potential risks on a site.

Nothing in these guidelines shall be construed as negating a contractor’s **statutory obligations** or requirements under any other enactments or regulations.

3. Security Risk Management (SRM)

The implementation of a Security Risk Management Process (SRMP) will provide a mechanism which ensures that security risks are managed on a systematic basis. This is achieved through the development of a documented and cohesive plan.

The SRMP shall include steps for:

1. the development of a SRM policy which identifies and documents responsibilities and commits to attaining;
 - (a) the security of people and property as required by the client,
 - (b) a safe and secure working environment.
2. the development of effective security and personnel procedures.
3. employee training and briefing.
4. procedures and controls to be monitored and reviewed.

Within this process contractors shall:

1. identify security risks;
2. assess the risk arising from all security risks identified;
3. prioritise the risks;
4. eliminate or control those risks; and
5. review risk assessments and control measures on a regular basis and immediately after an incident. This also applies to incidents that expose a person in the immediate vicinity to an immediate health or safety risk.

3.1 Identifying Risks

Risk identification relevant to a particular aspect of a contractor's operation (e.g. client's requirements, service provision, site, public interface, recorded incidents, command and control systems, etc) should be considered in the context of service provision as a whole.

Particular consideration shall be given to the location where the service is to be provided (e.g. residential, commercial, agricultural, etc) and the risk associated with such locations.

Attention should also be given to potential risks which could arise as a result of abnormal or

emerging situations (e.g. crowd dynamics, media interest, electrical/technical failures, weather alerts, traffic volumes, etc).

3.1.1 Risk Identification Process

The activities used to identify risks should include but are not limited to the following:

- consulting all relevant historical records relating to incidents;
- consulting client for whom service is being provided;
- consulting employees and/or others who provide the service;
- conducting assessments of site;
- conducting assessments of person(s) present/resident on site;
- conducting assessments of public interface;
- conducting assessments of crowd dynamics;
- conducting assessment of cultural behaviour;
- conducting assessments of access/egress points;
- assessing temporary structures and movable items;
- monitoring adherence to work procedures;
- determining training and skill levels, appropriate to the effective performance of duties;
- assessing the protection of people and property;
- assessing command and control systems;
- assessing vehicles and equipment and
- consulting with customers, An Garda Síochána, Government bodies, representative trade associations and risk assessment consultants on likely security risks.

Potential security risks shall be identified in respect of all aspects of the security service to be provided at the site. These aspects of operations shall include but are not limited to the following:

- the tasks performed;
- the location and surrounds involved;
- procedures;
- the building/structure;
- the assets to be secured;
- persons present including residents, workers, members of the public;
- any resistance to the service taking place;
- the different roles of the staff;
- the role of sub-contractors;
- the communication methods used;
- the time of day that the work is to be performed;
- use of Personal Protective Equipment (PPE);
- any other equipment or technologies required;
- work practices and procedures, shift working arrangements and other fatigue and stress

related risks;

- manual handling tasks;
- environmental factors (e.g. outdoor, terrain, weather, lighting, traffic and pedestrian flow, intoxication, exposure to blood and other bodily fluids, etc).

3.2 Assessing the Security Risk

After the identification of a risk, the contractor shall assess the risk posed by the risk. This informs the likelihood of an identified risk leading to an incident and the severity of consequence should an incident occur.

3.2.1 Security Risk Assessment

All security risk assessments shall be conducted by a person with appropriate skills and experience in health and safety, security risks and in risk assessment. The assessment shall be conducted in consultation with clients or their nominated representative, employees or other persons involved in the provision of security services.

The risk assessor shall ascertain and take into account (at a minimum) the following factors:

- known risks;
- adequacy of communication systems;
- compliance with regulatory requirements;
- efficacy of PPE for the tasks;
- environmental conditions;
- previous incidents which have occurred;
- site location, structures on site and layout;
- assets being secured;
- persons present;
- any resistance to the service taking place;
- staffing levels required to safely perform the work;
- technical equipment and other hardware;
- type of service required (taking account of public interface and crowd numbers, if applicable).

Factors that shall be taken into consideration when developing systems for the management of risks include but are not limited to:

- the outcome of the security risk assessment;
- information provided by clients and other third parties which may be relevant;
- command and control systems;
- availability of external resources (Gardaí, Fire, Ambulance, Local Authority);
- factors contributing to fatigue and stress (e.g. hours of work, time of day, shift length, number of rest breaks, amount of time between breaks, potential or actual exposure to

- workplace violence);
- the level of skill and experience of the staff carrying out the work;
- backup services including availability of additional staff and resources.

3.2.2 Establishing the Priority of Risks

Once the risks have been assessed the next step is to prioritise them for remedial action. All risks shall be dealt with in an appropriate manner and as soon as possible. While a high level of risk is the priority for corrective action, any medium or low level risk should not be ignored.

Contractors will be required to follow a four stage approach in prioritising risks:

Stage 1. Determine the likelihood of a risk related incident occurring.

Stage 2. Should an incident occur, determine its consequences and severity.

Stage 3. Combine the results of stages 1 and 2, to rate the level of the risk. The Risk Assessment Matrix set out at page 9 provides a template of how this should be recorded.

Stage 4. Prioritise the risks according to the outcomes of stage 3. This priority will be used in compiling and implementing a risk control plan.

3.3 Eliminating, Diminishing and Managing Risk

The risks identified and the assessment of the level of risk will determine the steps taken to manage those risks. The goal of the steps taken should be to eliminate or sufficiently manage the risk. These steps should not result in the creation of additional risks. Notwithstanding the obligation of contractors to comply with the PSA Requirements Document, consideration should be given to the following when setting risk mitigating and control measures in a risk control plan.

3.3.1 Elimination of Risk

The primary measure which should always be considered is the elimination of the risk. Notwithstanding the desirability of introducing a measure which completely eliminates the risk, one of the following risk management or control processes shall be undertaken where elimination of the risk is not possible.

3.3.2 Substitution of Risk

Replace the risk with one which carries a lower level of risk.

3.3.3 Risk Isolation

Isolate the risk, and in so doing prevent exposure to the risk.

3.3.4 Minimizing Exposure to Risk

The exposure to the risk may be reduced through:

- Engineering means or
- Administrative means or
- The appropriate use of PPE.

Examples of measures which may be used to manage risk include but are not limited to:

- Staffing levels;
- Equipment or technologies used for the protection of personnel and valuables;
- Implementation, development and adherence to secure work practices;
- Communication methods;
- Supervision;
- Training; and
- Command and Control systems.

3.4 Monitoring and Reviewing the Plan

Management of risks is an ongoing, evolving process. It is a cornerstone of business management and as such should be checked and reviewed periodically and as circumstances dictate. The process of identification, assessment and determination of control measures should be repeated when risk assessments and risk management measures are being reviewed. All those who are potentially affected by the change shall be consulted during the risk management process and informed of new requirements at completion.

4. Risk Assessment Template

The template on page 50 provides a basic format for all risk assessments referred to and required within the Requirements Document. A contractor may substitute another format for the risk assessment provided it has, as a minimum, the headings provided in the template. The template will assist contractors to:

- identify the risks,
- assess the level of risks,
- prioritise the risks and
- control and manage the risks.

A table shall be completed for each task and element of the security service being provided and should contain a comprehensive list of all identified risks and consequent assessed risks associated with each of those tasks and elements within the service provision. Please note that the five rows shown here are for illustrative purposes only and more may be added as appropriate.

Security Risk Assessment Methodology

Section 1: Context

1.1 Site Details

Client Name			
Site name			
Site location			
Name of assessor		Date of assessment	
Status (Draft/Final)			

1.2 Scope

An overview of the purpose of the report.

1.3 Purpose

Details as to why the report is required, it's aspirations or desired outcomes, who contributes and who sees the final document

1.4 Methodology

Details on how information relied upon for the report was gathered, this is completed last when the methodology is clear

1.5 Available Information

A well detailed section documenting all information currently available, including commentary on the premises location, the physical environment and structure, persons known to be on the premises, etc..

Section 2: Risks and Solutions

2.1 Risk Identification

Details of all risks including the origin of the risk and the consequences of events if the hazard/risk were to materialize. Risks should be placed in order of priority (This section can be expanded as required)

Priority	Risk Identified	Severity	Consequences

2.2 Controls

Details of recommendations/countermeasures proposed and reasons why, with comments on feasibility or restrictions/impediments. (This section can be expanded as required)

Priority	Risk Identified	Control	Reasoning

Section 3: Risk Analysis and Evaluation

LVI Table Matrix

Rating	Likelihood	Vulnerability	Impact
1	Extremely Improbable - A incident could only occur in extreme circumstances.	Very low – The business has more than adequate risk controls currently in place with redundancy and training in place.	Negligible - Slight or no disruption to business operation. No risk of harm.
2	Improbable – An incident may occur if other factors were present, but the risk is minimal.	Low - The business has more than adequate controls currently in place but without redundancy or training in place.	Slight - Minor delay to operations, minor asset damage, emotional impact to staff.
3	Possible – An incident may occur in conjunction with other factors.	Medium - The business has some risk controls in place however they are not adequate and require supporting measures.	Moderate – Operations delayed or disrupted. Moderate asset damage. Physical harm or psychological harm to staff.
4	Probable - An incident will most likely occur in the absence of further controls.	High – The business has minor risk controls in place however there are serious deficiencies in the adequacy of this controls.	Serious - Operational failure. Serious asset damage. Serious injury to staff.
5	Highly Probable – An incident will certainly occur in the absence of further controls.	Very High - There are no risk controls in this area or serious aggravating risk factors in place.	Very Serious – Operational failure, critical asset damage, death or serious injury to staff.

Risk Rating

Category	Score	Description
Critical	66 -125	Immediate action essential to address a specific security vulnerability
High	36 - 65	Immediate action recommended for effective security provision
Medium	11 - 35	Action recommended for a comprehensive security provision
Low	0-10	Currently controlled

Risk Assessment Template

Risk Assessment Template											
Asset/Activity	Threat	Risk Description	L	V	I	R	Recommended Controls	L	V	I	R

KEY to TEMPLATE:

L = Likelihood of risk occurring (rating is within the range of 1 to 5 with 1 being the least likely to occur and 5 being the most likely to occur) V = Potential Vulnerability (rating is within the range of 1 to 5 with 1 being the least vulnerable and 5 being the most vulnerable)

I = Impact (rating is within the range of 1 to 5 with 1 being the least impact and 5 being the greatest impact)

R = (this is arrived at by multiplying the numerical values assigned to likelihood, vulnerability and impact respectively as above). $L \times V \times I = R$ on a scale of 1 to 125 with 125 being the highest risk.

ANNEX C Cash Flow Template

Cash Flow Statement From												To													
Cash In	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12	Cash Out	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6	Month 7	Month 8	Month 9	Month 10	Month 11	Month 12
Sales																									
Own Funds																									
Loans																									
Overdraft																									
Other Incomings																									
Total Cash In																									
Sales Costs																									
Rent																									
Insurance Costs																									
Wages																									
Equipment Costs																									
Uniform Costs																									
Overheads																									
Loan Repayments																									
Tax																									
<ul style="list-style-type: none"> • Employer PAYE / PRSI • Income / Corporation Tax • VAT 																									
Other Outgoings																									
Total Cash Out																									
Cash Flow: Surplus/(Deficit)																									
Opening Cash Balance																									
Closing Cash Balance																									

Annex D Audit Report

PSA 91:2023 - CONTRACTOR DETAILS					
1. Name of Contractor					
2. Address on PSA Licence					
3. Address where Audit Took Place (if different from address at 2 above)					
4. Phone No.		5. Email Address			
6. Contact Person			7. PSA Licence No		
PSA 91:2023 – Section 3. Organisation					
Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>3.1 Ownership</u>					
3.1.1 Names and contact details of each person to be recorded:					
3.1.3 Names and contact details of all directors and company secretary to be recorded:					

PSA 91:2023 – Section 3. Organisation

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Screening Requirements Met:					
3.1.4 Evidence of compliance with competency requirements met					
3.1.5 Details of former businesses, directorships, partnerships, or sole trades etc. of directors reviewed					
3.1.6 Details of any bankrupt person:					
3.1.7 Details of any beneficial interest in another organisation:					
3.1.8 Details of any person who is a beneficiary of the organisation					

PSA 91:2023 – Section 3. Organisation

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
3.1.9 Copy of organisation chart provided where not previously supplied at Pre-Audit checklist:					
3.1.10 All directors, management, supervisory and operational staff hold the required employee licence:					
<u>3.2 Finances</u>					
3.2.1 TCC inspected: TCC No: Issue Date: Expiry Date:					

PSA 91:2023 – Section 3. Organisation

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<p>3.2.2 Details of any director or shareholder loans:</p> <p>Date of Loan:</p> <p>Amount of Loan:</p> <p>Who the Loan is From:</p> <p>Amount of repayments made:</p> <p>Date of repayments:</p> <p>Amount of Loan Outstanding:</p>					
<p>3.2.3 Cash Flow Statement inspected:</p> <p>Copy Provided:</p>					

PSA 91:2023 – Section 3. Organisation

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>3.3 Insurance</u>					
3.3.1 Details of Insurance:					
3.3.2 Details of sufficient funds 3 times the value of the excess amount available :					

PSA 91:2023 – Section 3. Organisation

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Requirement that Funds held in a separate organisation's operational account :					
3.3.3 Confirmation provided that the organisation does not self-insure in whole or part.:					
<u>3.4 Premises</u>					
3.4.1 All records, etc. stored in secure confidential manner:					

PSA 91:2023 – Section 3. Organisation

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
3.4.2 Details of intruder alarm:					
3.4.3 Details of Alarm Monitoring					
<u>3.5 Organisation Information</u>					
3.5.1 PSA Licence Number(s) contained on letterheads, contracts, etc.: Details of any unlicensed activity:					

PSA 91:2023 – Section 3. Organisation

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
3.5.2 Written contracts inspected and required details included therein					
3.5.3 Contracts signed and delivered to client as required:					
3.5.4. Details of sub-contractor(s) including PSA licence number and expiry date:					

3.6 Quotations in pursuance of Contracts or Business

PSA 91:2023 – Section 3. Organisation

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
3.6.1 Written quotation comply with requirements:					
3.6.2 Written documentation includes the total cost for the service and method of payment:					
<u>3.7 Compliance with Legislation</u>					
3.7.1 Statement on compliance with legislation provided: Meets all requirements of 3.7.1:					
3.7.2 Statement on compliance with pay and conditions agreements/legislation:					

PSA 91:2023 – Section 3. Organisation

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Verified compliance with 3.7.2					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>4.1 Selection and Pre-Employment Screening</u>					
4.1.1 General					
4.1.1.1 Pre-employment records inspected: Required enquiries completed:					
4.1.1.2 Required screening undertaken:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
4.1.1.3 Required personnel files exist					
4.1.1.4 Statements of Authorisation on files:					
4.1.1.5 No applicant offered relevant employment without holding a PSA Licence and having completed the screening process					
4.1.1.6 Provisional Employment time frame meets requirements:					
4.1.1.7 Certified copies of personnel and screening documentation on file:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
4.1.1.8 Screening records for part-time employees and directors inspected:					
4.1.1.9 Screening records for temporary & ancillary staff inspected: Screening completed:					
4.1.1.10 Screening periods complied with:					
4.1.1.11 Age requirements complied with:					
4.1.1.12 Age requirements complied with: Number of Staff aged over 65:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Fitness for duty certificate(s) provided:					
4.1.1.13 Monitoring & supervision procedures for provisional employees in place:					
4.1.1.14 Screening completed within 13 weeks of employment commencing:					
4.1.1.15 Screening for shorter periods carried out in accordance with PSA requirements:					
4.1.1.16 Gaps in screening records have been covered in accordance with PSA requirements:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
4.1.2 Pre-Employment Interview					
4.1.2.1 Pre interview documents provided:					
4.1.2.2 Interview conducted to the requirements of PSA 91:2023:					
4.1.2.3 Interview notes recorded in line with PSA 91:2023 requirements set out in 4.1.2.2 shall be taken by the organisation and retained on personnel file of the applicant.					
4.1.3 Character and Other References					
4.1.3.1 Screening procedures complied with:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
4.1.3.2 Procedures for references by phone followed:					
4.1.3.3 Requirements on third party documents met:					
4.1.3.4 Where records are not available requirements are met:					
4.1.3.5 Where there are gaps in the career record which cannot be independently confirmed in accordance with the written verification procedures:					

4.1.4 Evidence of Qualifications/Awards

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
4.1.4.1 Evidence of qualifications/awards received: PSA Licence details provided prior to employment:					
4.1.5 Work Permits, Authorisations and Permissions					
4.1.5.1 All permissions in place prior to employment commencing:					
4.1.5.2 Register of employees in place and in line with PSA requirements: Current permissions are in place:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
4.1.5.3 Register held on site as required :					
4.1.6 Maintenance and Retention of Records					
4.1.6.1 All PSA required employee details held on file:					
4.1.6.2 Storage of Records secure: Records retained in accordance with Data Protection Commissioner:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
4.1.6.3 List of personnel maintained:					
4.1.7 Screening and Acquired Companies					
4.1.7.1 Screening requirements for employees met:					
<u>4.2 Terms of Employment</u>					
4.2.1 Contract of employment and staff handbook issued to staff:					
4.2.2 Terms of employment inspected and meet PSA requirements:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>4.3 Code of Conduct</u>					
4.3.1 Code of conduct meets PSA 91:2023 requirements:					
4.3.2 Code of conduct signed by employees:					
<u>4.4 Licence Card</u>					
4.4.1 All Enforcement Managers and Enforcement Guards have a valid PSA licence card:					
4.4.2 instructions on the use of PSA Licence card given to employees:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>4.5 Uniform</u>					
4.5.1 Uniform complies with PSA requirements:					
4.5.2 Uniform complies with colour and lettering requirements of PSA 91:2023:					
4.5.3 Uniform distinguishable from civil protection services:					
4.5.4 Uniform contains unique identity Number:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
4.5.5 Organisations insignia clearly visible:					
4.5.6 All personnel aware that their facial feature should be clearly visible at all times:					
4.5.4 Procedures for renewal of uniforms:					
4.5.8 Uniform cost is borne by organisation:					
4.5.9 Procedures in place for recoup of uniform cost where an employee leaves an organisation and the uniform is not returned:					
4.5.10 A record of all uniforms not returned retained by the organisation:					

PSA 91:2023 – Section 4. STAFFING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>5.1 Training Policy and Responsibility</u>					
5.1.1 Training Policy document inspected and PSA requirements met:					
5.1.2 Details of Training Administrator:					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Qualifications:					
5.1.3 Verified Training records inspected and in accordance with PSA requirements:					
5.1.4 Policy to include Assessment of operational staff including additional training where required:					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>5.2 Induction Training</u>					
5.2.1 Details of Induction Training records inspected: Meets PSA requirements: 5.2.2 Training provided prior to commencing operational duties: 5.2.3 Training provided by competent member of staff:					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>5.3 Specialist Training</u>					
5.3.1 Specialist training provided in line with PSA requirements:					
5.3.2 Specialist training provided in line with PSA requirements:					
<u>5.4 Refresher Training</u>					
5.4.1 1 Refresher training records inspected: Meet PSA requirements					
<u>5.5 Supervisory and Management Training</u>					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
5.5.1 Supervisory & Management training records inspected: Meet PSA requirements					
<u>5.6 Training Records</u>					
5.6.1 Training records inspected & maintained:					
5.6.2 Training Records meet PSA requirements :					
5.6.3 Verification of all training available for inspection :					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
5.6.4 All refresher training recorded and the record held and retained on the employee's personnel file by the employer:					
5.6.5 Records indicate where further training is required:					

PSA 91:2023 – Section 6. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>6.1 Risk Assessments</u>					
6.1.1 and 6.1.2 Risk Assessment survey documentation inspected:					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Surveys undertaken for each site: Meet PSA requirements:					
6.1.3 Security Management Plan inspected : Meets PSA 91:2023 Requirements :					
6.1.4 Body Cameras used in line with PSA 91:2023 requirements:					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<p>6.1.5 Data Protection Impact Assessment on the use of body cameras completed:</p> <p>Declaration form the Data Controller of the organisation to confirm that use of body cameras meet data protection provisions:</p>					
<p>6.1.6 Body Camera User Policy inspected:</p> <p>Meets PSA 91:2023 requirements:</p>					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.1.7 Enforcement guard instructed on operational use of body cameras:					
6.1.8 Policy in place for when cameras are not being used : Confirmed storage in a safe and secure facility with access restricted to designated officers of the organisation as identified in DPIA.					
6.1.9 Training on use of body cameras provided prior to any operation:					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Meets requirements of PSA 91:2023					
6.1.10 Numbers of ENF Guards on duty in accordance with Risk Assessment and Security Management Plan:					
6.1.11 Number of ENF Guards on duty meet requirements of PSA 91:2023					
6.1.12 Pre-operation briefing sessions held at a sites other than the project sites:					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.1.13 Verification that written assignment instructions on duties and responsibilities issued to ENF Guards and Sub-contractors:					
6.1.14 Attendance Register inspected:					
6.1.15 Copy of Register attached to the Security Management Plan.					
<u>6.2 Times and Hours</u>					
6.2.1 Enforcement Guards services provided at appropriate times/days, considering religious or cultural observance:					

PSA 91:2023 – Section 5. TRAINING

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.2.2 Time restrictions on service provision observed:					
<u>6.3 Mode of entry</u>					
6.3.1, 6.3.2, 6.3.3 & 6.3.6 Modes of entry used by Enforcement Guards met PSA 91:2023 requirements:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>6.4 Goods</u>					
6.4.1 , 6.4.2 & 6.4.3 Goods seized in accordance with the requirements of PSA 91:2023:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.4.4 The list of goods removed verified:					
<u>6.5 Vulnerable situations</u>					
6.5.1 & 6.5.2 Guidelines in place for dealing with persons identified as vulnerable or underage:					
<u>6.6 Enforcement Manager</u>					
6.6.1 Enforcement Manger appointed : Position within the organisation:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.6.2, 6.6.3, 6.6.4, 6.6.5 & 6.6.6 Enforcement Manager declaration confirms compliance with all PSA legislation, regulations and requirements during the provision of the security service:					
<u>6.7 Command and Control Systems</u>					
6.7.1 Command & Control facilities meet PSA requirements:					
6.7.2 Confirm status of command and control system (dedicated, contracted or shared) Clients advised of system(s):					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Site/Mobile system used: Looped check-in-call systems used: Meet PSA requirements:					
6.7.3 Minimum provisions for command and control systems met:					
6.7.4 Dedicated fixed location visited: Meets PSA requirement:					
6.7.5 Report on contracted facilities inspected: Meets PSA requirements: Facility					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.7.6 Command & Control System accessed:					
<u>6.8 Incident Reporting</u>					
6.8.1 Identity of Enforcement Manager or other reporting staff made available in writing to all operation staff:					
6.8.2 All Incidents handled by the Enforcement Manager recorded: Incident report details meet PSA Requirements:					
6.8.3. Facilities in place meets the PSA Requirements:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.8.4 Escalation Policy in place for client liaison:					
6.8.5 Records of all incidents are maintained in accordance with PSA Requirements: Details meets PSA Requirements:					
<u>6.9 Threats and Violence</u>					
6.9.1 Risks of violence assessed:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Mitigating measures implemented per 6.1:					
6.9.2 Mitigating measures implemented:					
6.9.3 Special training and safety routines in place where required:					
6.9.4 Tasks involving a high risk of violence identified in the risk assessment: meets the requirements of 6.1.5:					
6.9.5 Incidents involving violence recorded:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
Meets PSA Requirements:					
6.9.6 Appropriate physical and psychological support available, on request, to any employee who has been subjected to violence as a result of carrying out his/her duties:					
<u>6.10 Operations Records</u>					
6.10.1 Operation records inspected: Meets PSA Requirements:					
6.10.2 Facilities in place to meet PSA Requirements:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<u>6.11 Assignment Instructions</u>					
<p>6.11.1 Assignment Instructions inspected:</p> <p>Meet PSA requirements:</p>					
<p>6.11.2 Requirements for endorsement met:</p>					
<p>6.11.3 Assignment instructions available in the security management plan and a copy shall be available to the client:</p>					
<p>6.11.4 Assignment instructions include required details:</p>					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.11.5 Each Enforcement Guard received individual assignment instructions which included the required detail:					
<u>6.12 Security of Information and Access Media</u>					
6.12.1 Routines established to deal securely with information:					
6.12.2 Procedures in place ensuring appropriate level of access to clients details:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<p>6.12.3 Procedures in place to ensure client details are not made known to a 3rd party unless with written permission:</p> <p>Written Permission verified:</p>					
<p>6.12.4 Back-up & Storage procedures in place:</p> <p>Meet PSA Requirements:</p>					
<p>6.12.5 Procedures for the surrender of key meet PSA Requirements:</p>					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.12.6 Retention and Storage of data complies with Data Protection Legislation:					
6.12.7 Report to the client on any un-executed orders/warrants:					
<u>6.13 Vehicles and Equipment</u>					
6.13.1 Vehicles liveried in accordance with PSA Requirements:					
6.13.2 Vehicles contain two way communication capability: Fire extinguisher: First aid kit:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
6.13.3 Driving licences valid: Copies held on employees files:					
6.13.4 river History forms maintained and verified in line with PSA requirements:					
6.13.5 Vehicle distinguishable from civil protection and emergency vehicles:					
6.13.6 Cleary defined instructions on roles provided to drivers: Meets PSA Requirements:					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<p>6.13.7 Vehicles and equipment serviced and maintained:</p> <p>Records inspected:</p>					
<p>6.13.8 Equipment signed for:</p> <p>Undertaken to return equipment:</p>					
<p><u>7.1 Compliance with Standards</u></p>					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
<p>7.1.1 1 Has organisation maintained compliance with standard:</p> <p>Instances of non-compliance not recorded elsewhere in audit report:</p> <p>Any other matter to be brought to the attention of the PSA:</p>					
<p>7.1.2 Duration since last audit:</p> <p>If greater than 12 months reasons for same:</p>					

PSA 91:2023 – Section 7. OPERATIONS

Requirement	Outcome	Action required?	Date When Compliance To Be Achieved	Action Completed?	Verified and how verified?
7.1.4 Has organisation provided all required permissions:					
<u>7.2 PSA Licensing Requirements</u>					
7.2.1 Not Applicable					
7.2.2 & 7.2.3 Compliant with all relevant legislation :					
7.2.4 Statement on notifying the PSA of certain matters provided: Copy attached to the report:					

PSA 91:2023 – INTERNAL AUDIT REPORT SUMMARY

PSA 91:2023 – INTERNAL AUDIT REPORT SUMMARY						
8. No of Non-Conformances Recorded	CAT 1	CAT 2	CAT 3	9. Date(s) of Previous Audit		
10. Summary of Non-Conformances Found	Clause Ref.	Category of Non-Conformance	Non-Conformance Addressed? (Y/N)	Date Compliance Achieved?	Inspector Comment	
11. Other Information of Relevance, if applicable						

Inspector:

Date:

**The Private
Security Authority**

Davis Street
Tipperary Town
Co. Tipperary
E34 PY91
T: 062-32600
E: info@psa.gov.ie