BS 8507-1:2008

BSI Standards Publication

Code of practice for close protection services –

Part 1: Services within the United Kingdom

bsi.

...making excellence a habit.™

Publishing and copyright information

ISBN 978 0 580 58560 9

ICS 13.310

The following BSI references relate to the work on this standard:
Committee reference GW/3
Draft for comment 08/30163414 DC

Publication history

First published November 2008

Amendments issued since publication

Amd. No.	Date	Text affected

Contents

Summary of pages
This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 18, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI and came into effect on 30 November 2008. It was prepared by Technical Committee GW/3, *Manned security services*. A list of organizations represented on this committee can be obtained on request to its secretary.

Information about this document

Attention is drawn to the Private Security Industry Act 2001 [1], which contains provisions for regulating the private security industry, including close protection. A person falling within the definition of providing security industry services under the Private Security Industry Act 2001 [1] is required to be licensed in accordance with that Act. The Act can be found online at http://www.the-sia.org.uk

Attention is also drawn to the Data Protection Act 1998 [2], the Disability Discrimination Act 1995 (as amended) [3], the Human Rights Act 1998 [4], the Race Relations Act 1976 [5], the Rehabilitation of Offenders Act 1974 [6] and the Sex Discrimination Act 1975 [7]. If there is any inconsistency between this British Standard and any domestic legislation, then the legislation prevails.

Use of this document

As a code of practice, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this British Standard is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should".

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

The word "should" is used to express recommendations of this standard. The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Notes and commentaries are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations. Commentaries give background information.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This page deliberately left blank

1 Scope

This British Standard gives recommendations for the management, staffing and operational accountability for the provision of all aspects of close protection services within the United Kingdom of Great Britain and Northern Ireland, and Crown Dependencies. Additionally, this code might be used by those who wish to purchase close protection services.

NOTE Recommendations for operations in other territories outside the United Kingdom are given in BS 8507-2[1)].

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 7858, *Security screening of individuals employed in a security environment – Code of practice*

BS ISO 10002, *Quality management – Customer satisfaction – Guidelines for complaints handling in organizations*

3 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1 client

person or organization requesting the service

3.2 close protection operative (CPO)

person with specialized training who performs close protection services

3.3 close protection services

services to establish and maintain a safe environment for a principal at risk

3.4 principal(s)

person or persons being afforded protection

3.5 risk assessment

continuous process of collection, collation and analysis of information to identify possible danger(s)

1) In preparation.

3.6 service provider

person or organization providing services to the client

3.7 sub-contractor

person or organization providing close protection services under the direction of the service provider

3.8 team leader

competent person nominated to take charge of and be responsible for a team of CPOs and to provide liaison between the team, the principal or client and the service provider

3.9 threat assessment

ongoing evaluation of threats and vulnerabilities to determine the possibility, nature and level of danger, harm or loss to the principal

4 Service provider

4.1 Structure

The service provider should possess a clearly defined management structure showing control and accountability at each level of operation.

The service provider should operate a complaints management system in accordance with the guidance given in BS ISO 10002.

Details of the senior manager or executive officer responsible for the operations should be established and a curriculum vitae made available to prospective clients on request. Also details of the owner of the service provider should be made available. Any unspent criminal convictions or undischarged bankruptcy of the executive officer or owner should be disclosed on request.

NOTE Attention is drawn to the Rehabilitation of Offenders Act 1974 [6], whose provisions govern such disclosure.

4.2 Finances

The service provider should have sufficient working capital for its requirements. The capital reserves of the service provider should be sufficient for current and planned needs.

The service provider should be able to present two years' certified trading accounts, except if it is starting as a subsidiary of an established service provider. Alternatively the service provider should be able to provide evidence that staff experience and financial backing are commensurate with the level of trading.

The service provider should prepare annual accounts in accordance with applicable accounting standards. The accounts should be certified by an accountant. Accounts should be available on request for agencies, organizations or individuals with an appropriate interest in the bona fide nature of the service provider.

4.3 Insurance

The service provider should possess insurance cover commensurate with the services provided and the number of persons employed, e.g. public liability, contractual, efficacy, employer's liability, vehicle insurance and fidelity guarantee.

Where a service provider uses sub-contract staff, the service provider should ensure there is sufficient insurance cover commensurate with the business undertaken.

5 Resources

5.1 Premises

The service provider should have an administrative office(s) and/or operational centre(s) where records, professional and business documents, certificates, correspondence, files and other documents necessary for conducting business transactions should be kept in a secure manner. The location of records and documentation, both local and centralized, should be clearly defined by the service provider.

5.2 Directly employed staff

5.2.1 Selection and screening

All persons undertaking, or having access to, details of close protection duties should be selected and screened in accordance with BS 7858.

If employees are acquired through a takeover, the service provider should satisfy itself that the recommendations of this subclause have been fully met.

They should also be able to demonstrate appropriate skills in reading, writing and verbal communication sufficient to perform their roles effectively.

Prospective employees should be asked to confirm that there is nothing in their circumstances that would be detrimental to their operational commitments.

5.2.2 Health

The service provider should ensure that the health and physical condition of personnel remains compatible with the duties to which they will be deployed.

NOTE Where health and safety risk or medical concerns of personnel are raised, it is reasonable for a service provider to ask that person to undergo a medical examination to ensure fitness for duty.

5.2.3 Terms and conditions of permanent staff

Employees should receive a written statement (e.g. handbook) of the terms and conditions of their employment that include details of the following:

a) job title;
b) effective start date;
c) probationary period (if required);
d) provisional period subject to screening (if applicable);
e) pay and allowances;
f) hours and days of work;
g) leave entitlement;
h) conditions of payment during absence through illness;
i) pension entitlement;
j) industrial injury procedures;
k) the address of the service provider;
l) disciplinary and appeals procedures;
m) terms of notice of termination of employment;
n) confidentiality agreement;
o) equality and diversity policy/procedure;
p) performance review policy/procedure.

Persons should not be required to work hours that could be detrimental to their health, safety or efficiency.

NOTE Attention is drawn to statutory requirements relating to employment, and in particular, to requirements relating to working hours.

5.2.4 Code of conduct

NOTE This list is not exhaustive and does not necessarily include all actions that could also constitute criminal offences.

All personnel should be issued with a code of conduct and instructed that the following (including the aiding and abetting of others) constitute a breach of the code of conduct:

a) neglecting to complete a required task at work promptly and diligently, without sufficient cause;
b) leaving a place of work without permission, or without sufficient cause;
c) making or signing any false statements, of any description;
d) destroying, altering or erasing documents, records or electronic data without permission or through negligence;
e) divulging matters confidential to the service provider, client or principal, either past or present, without permission;
f) soliciting gratuities, or not reporting gifts received, or other consideration from any principal or principal's representative;
g) failure to exercise reasonable care of, or properly account for, keys, money, property or information (e.g. principal's itinerary) received in connection with business;
h) incivility to persons encountered in the course of duties, or misuse of authority in connection with business;
i) conduct in a manner likely to bring discredit to the service provider, principal or client;

j) use of equipment or identification without permission;

k) reporting for duty under the influence of alcohol or restricted drugs, or use of these whilst on duty;

l) failure to notify the employer immediately of any:

1) conviction for a criminal offence including a motoring offence carrying endorsement or fixed penalty;

2) police caution;

3) refusal, suspension or withdrawal (revocation) of a Security Industry Authority (SIA) licence, if appropriate.

NOTE For definitions see the SIA website.

m) permitting unauthorized access to a principal's or client's premises;

n) carrying of unauthorized or unlawful equipment, or use of a principal's equipment or facilities without permission;

o) solicitation of contracted personnel, client or principal;

p) failure to disclose any circumstances that can involve a conflict of interest (e.g. between themselves and the client or the principal).

5.2.5 Licensing status

A record of the current status of SIA and other relevant licences should be maintained and regularly reviewed.

Regular checks should be carried out to confirm that CPOs requiring SIA licences comply with the terms and conditions of their licence at all times.

5.3 Sub-contractors

*COMMENTARY ON **5.3***

It is recognized that the vast majority of CPOs are sub-contractors.

5.3.1 General

Service providers should ensure that they have appropriate written contractual arrangements in place with sub-contractors.

5.3.2 Initial selection and screening

NOTE In parts of the United Kingdom where licensing by the SIA is not mandatory by law, service providers can seek further advice on security screening from BS 7858.

Although no system of selection can provide absolute security, providers of close protection services should make every endeavour to ensure that the integrity and quality of its CPOs is established and maintained.

The service provider should carry out relevant pre-employment enquiries to ensure that only suitably skilled sub-contractors are recruited or added to a database. The service provider should hold curricula vitae for all CPOs on the service provider's database.

The initial selection procedure should include a personal interview and should be designed to assess the following:

a) physical ability to carry out the services required;

b) aptitude and demeanour;

c) literacy and verbal communication abilities;

d) personal documentation (proof of name, age, address, SIA licence, etc.);

e) details of SIA-approved qualifications, other training and additional skills.

The service provider should require the applicant to provide an up-to-date curriculum vitae including:

1) details of career history of not less than five years immediately prior to the date of the application or back to the date of ceasing full-time education;

2) the names of at least two persons, who may be former employers, from whom a reference can be obtained.

The initial screening should be completed within six weeks and should be considered valid for up to one year from completion of screening.

5.3.3 Subsequent screening

Subsequent screening should be carried out at least annually and should include a signed declaration from the sub-contractor detailing any relevant changes in personal and professional circumstances (e.g. training undertaken, qualifications obtained).

NOTE For an example declaration, see Annex A.

5.3.4 Suppliers of sub-contract labour

Employers of sub-contract labour should also follow the recommendations given in **5.3**, **5.4** and **5.5** of this standard. The service provider should satisfy itself that these recommendations have been followed.

5.3.5 Qualifications of sub-contractors

The service provider should satisfy itself that sub-contractors:

a) are satisfactorily screened in accordance with BS 7858 or in accordance with **5.3.2**;

b) are competent to undertake the work involved;

c) are adequately insured;

d) have individually signed a confidentiality agreement relating to the disclosure of the client's and the service provider's confidential information or material;

e) agree to report immediately to the service provider any alleged or actual contravention of United Kingdom law;

f) are appropriately licensed by the SIA.

Evidence of items a) to f) above should be retained by the service provider.

5.4 Equipment

5.4.1 Vehicles

Operational vehicles should:

a) be appropriate for their intended use;

b) carry appropriate communication equipment to meet operational requirements;

c) be inspected by the CPO prior to use to ensure that they are roadworthy, legal and operationally effective;

d) be serviced regularly, in accordance with the manufacturer's instructions.

Any damage or defects to operational vehicles including third party vehicles should be reported as soon as possible.

The service provider should hold on file six-monthly authenticated versions of the most up-to-date copies of driving licences where permanent employees are required to drive on business purposes.

5.4.2 Other equipment

All equipment used by or supplied to CPOs should be appropriate to meet operational requirements.

The service provider should have documented procedures in place to ensure control, and availability, of equipment held by the service provider.

All equipment should be appropriately maintained and should meet legislative and regulatory requirements.

5.5 Training

5.5.1 General

The service provider should have a clearly defined and documented training policy.

5.5.2 Induction training

NOTE The content, timing and duration of induction training are left to the discretion of the service provider.

The service provider should provide induction training in matters related to conditions of employment and organizational procedures for all employees. This induction training should be additional to the role-specific close protection training described in **5.5.3**. Induction training for directly employed staff should be provided prior to operational duties.

5.5.3 Role-specific training

The service provider should ensure that all CPOs, whether directly employed or sub-contracted to provide close protection services, have received role-specific training.

NOTE 1 This would normally be confirmed by the CPO holding the appropriate SIA licence if operating in the UK.

Where the CPO is not required to hold the SIA licence, they should provide proof of their training, which should be equivalent to, or greater than, the content and level specified in the current SIA Specification for Core Competency Training and Qualifications for Close Protection Operatives [8].

All training should provide the CPO with knowledge and skills to provide an effective close protection service.

NOTE 2 Further advice and information on appropriate training can be obtained from the UK Awarding Bodies who are approved by the SIA to award the qualification for licensing for close protection.

5.5.4 Specialist training

CPOs required to perform specialist duties in the UK (e.g. advanced driving, surveillance, advanced first aid, electronic counter-measures, threat assessment, improvised explosive devices) should be trained to a proficient standard by suitably qualified persons. Training should be provided on the use of specialized equipment.

5.5.5 Operation familiarization

Where necessary for operational effectiveness, CPOs should be given appropriate familiarization training.

5.5.6 Operations control point training

Where an operation control point is used, e.g. by a residential security team, training and instruction of CPOs should include the following:

a) initial set-up;

b) outline of control point operations;

c) standard operational procedures;

d) location specific assignment instructions;

e) communications;

f) documentation and recording procedures (e.g. daily occurrence book);

g) safety and security of information;

h) emergency procedures;

i) duty rosters;

j) hand-over or take-over (if applicable);

k) point of contact list (client and CPOs).

NOTE This is not an exhaustive list.

5.5.7 Team leader proficiency

5.5.7.1 The service provider should ensure that CPOs who have team leader responsibilities are able to demonstrate the skills and experience required in their relevant role, e.g. in the following areas:

a) leadership skills;

b) operational planning;

c) team management.

5.5.7.2 The service provider should ensure that a team leader understands the importance of:

a) reviewing the performance of individuals and the team;

b) ensuring the implementation of improvements;

c) recognizing achievements.

5.5.8 Refresher training

The service provider should monitor the effectiveness of all CPOs and, if necessary, refresher or remedial training should be provided by suitably qualified persons as soon as practicable.

5.5.9 Contingency training

If there is a change in methods, procedures or legislation, the service provider should ensure that CPOs are retrained to a proficient level by suitably qualified personnel. If practicable, training should take place before change is implemented.

5.5.10 Training records

Evidence of training and qualifications should be recorded and a copy retained.

5.6 Documents and data

Separate records (hardcopy or electronic) should be maintained for each client, principal, employee and supplier.

The records should be held in a secure manner, but should be easily accessible to authorized persons (see **5.3.2**).

Amended or updated records should be identifiable by date and clearly distinguishable from previous versions.

Information stored in an electronic retrieval system should be regularly backed-up. The back-up copies should be stored separately.

NOTE 1 Further information on the management of electronic data can be found in BS 7799-1 and BS 7799-2. Advice on the storage of electronic media can be found in BS 5454.

NOTE 2 Attention is drawn to provisions and requirements of the Data Protection Act [2].

Archived records should be clearly indexed.

All records concerning a contract should be maintained for at least 12 months after termination of the contract. Such records should include:

a) all issues of operation instructions;

b) incident reports;

c) details of persons employed on the operation;

d) briefings and debriefings.

An employee's basic records (as detailed in BS 7858) should be kept for at least 7 years from the cessation of their employment.

NOTE 3 Minimum periods for retention of records can be reviewed if applicable for particular purposes, especially with regard to potential liabilities for civil action.

6 Service

6.1 Sale of services

6.1.1 Client information

Where requested by a potential client, the service provider should be prepared to provide the following minimum information:

a) the name, address(es) and telephone number(s) of the service provider;

b) details of trade association or professional body membership(s);

c) proof of compliance with industry standards, or details of certification by a United Kingdom Accreditation Service accredited certification body;

d) legal entity of the service provider (e.g. public limited company, limited company, limited liability partnership or sole trader);

e) the registered number, address and date of registration if the service provider is an incorporated company, or details of partners and an address for legal service of documents if it is a partnership or sole trader;

f) proof of insurance;

g) data protection notification.

6.1.2 Contractual arrangements

A written quotation should be provided by the service provider. The quotation document should state:

a) the detailed and total costing for the service, and the arrangements for payment;

b) the contract period, along with procedures for termination of the contract;

c) any other contractual requirements made with the client;

d) terms and conditions.

The client should be asked to acknowledge acceptance of the quotation.

NOTE Due to the nature of the sector, a written contract might not always be available.

6.1.3 Contract records

Copies of records relating to the contractual agreement between the principal/client and the service provider should be retained in a client file. These records should be retained and controlled in accordance with **5.6**.

6.2 Due diligence

The service provider should ensure that they know the identity of the client requesting the service and that the client has an ethical and legitimate reason for requesting it.

6.3 Scope of task

6.3.1 Initial client requirements

The service provider should confirm details of the client's specific requirements (e.g. what service, who, when, where, how).

NOTE These may include but are not limited to threat, location(s), relevant points of contact, history.

6.3.2 Planning considerations

The service provider should consider the following when planning an operation:

a) threat and risk assessment (for an example, see Annex B);

b) principal profile;

c) selection of CPOs and allocation of responsibilities;

d) timeframes;

e) locations;

f) resources, communication and logistics;

g) liaison with relevant third parties;

h) special requirements (e.g. medical);

i) preparation of the operation plan.

6.3.3 Client's approval

The service provider should provide the client with recommendations and costing for their approval.

6.3.4 Implementation and ongoing monitoring

The operation plan should be issued, the team briefed and the plan implemented.

This should include continued monitoring of, and response to, the operational effectiveness of the service.

6.3.5 Completion of task

The CPO(s) should be debriefed and any action points noted and implemented. A record of this should be kept on the client's file.

Where practical, the client should be debriefed. A record of this should be kept on the client's file.

NOTE Attention is drawn to the Data Protection Act [2].

6.4 Threat and risk assessment

The service provider should ensure that initial threat and risk assessments are conducted by a competent person. These should identify specific operational risks to the CPO(s) and principal(s). A record of these assessments should be kept and used for the production of the operation plan.

NOTE An example of a threat and risk assessment can be found in Annex B.

The threat and risk assessment should be updated dynamically during the operation.

6.5 Briefing

All CPOs should be briefed in order to ensure that they understand the requirements of the operation.

A briefing should include information on the following:

a) objective of the operation;

b) levels of threat and risk;

c) resources and logistics;

d) operational methodology;

e) CPO roles and responsibilities;

f) administration and communications.

6.6 Conduct of operation

*COMMENTARY ON **6.6***

It is recognized that a team could comprise a single CPO, in which case the responsibilities of team leader and team member would belong to that single CPO.

6.6.1 Service provider

The service provider should:

a) maintain close liaison with the client or principal as required to ensure any changes that might effect the level of risk are communicated in a timely manner;

b) ensure the resources and control measures allocated to the operation remain appropriate to any change in the level of threat;

c) provide appropriate communications and support for the team leader during the operation.

6.6.2 Team leader

During the operation the team leader should:

a) maintain a safe environment for the principal;

b) ensure all team members and the principal are correctly briefed on any changes to the operation plan;

c) ensure all team members are conducting their duties competently;

d) plan the administration and oversee the welfare of the team (e.g. adequate refreshments and periods of rest);

e) ensure serviceability of all equipment, vehicles and other modes of transport issued and supplied (see also **5.4.1**, **5.4.2**).

6.6.3 Team member

A team member should:

a) conduct their duties competently;

b) inform the team leader as soon as is practical of any changes which might impact on the effectiveness of the operation.

6.6.4 Close protection operational debriefing procedure

6.6.4.1 General

Debriefs should occur at the end of each operation and, where necessary, at other key times during the operation.

6.6.4.2 Aim of debrief

The debrief should determine the effectiveness of the operation from the perspective of the operational team and, where possible, the principal and the client.

NOTE It is recognized that it is not always possible to debrief all team members, the principal or the client.

6.6.4.3 Scope of operational debrief

An operational debrief should include a review of all the key briefing factors. It should include a general overview of the operation involving all team members and should identify those areas that worked well and those that needed remedial action. Any comment/ feedback from the principal should be taken in to consideration as part of the debrief process.

It is important that notes of any key points should be made, and that any remedial action identified should inform future planning.

6.6.4.4 Client debrief

Consideration should be given to contacting the client for their feedback on any commercial and administrative aspects of the operation.

Annex A (informative) Sample sub-contractor declaration

Declaration of sub-contract close protection staff

Name:

SIA Licence Number:

Current Address:

Telephone Number:

E-mail address:

I hereby declare that since my last declaration I have not:

1) been convicted of a criminal offence (including motoring)
2) accepted a caution from Police
3) been bailed by Police
4) had a County Court Judgement registered against me
5) been made bankrupt or entered into an Individual Voluntary Arrangement
6) had my SIA licence suspended or revoked by the SIA.

Nor do I know of any other reasons which would make me unsuitable for performing the demanding role of a Close Protection Officer.

I attach an updated copy of my CV.

Signed: **Date:**

Print:

N.B. If any of the above have changed then do not sign this form but get in touch with us directly.

Continuing Professional Development

List here any relevant professional training which you have completed in this period.

Course	Dates	Qualification (if any)

Please supply copies of any relevant certificates

Annex B (informative) Sample client/principal threat and risk profile

NOTE This is not intended to be a definitive version and is intended to be an example only. Once this document has been completed it is recommended that it is given the relevant security classification and treated accordingly.

Threat and Risk Assessment		
Date:	**Completed By:**	
Client:		
Client's brief:		
Person(s) at risk		
Principal only; Family; Relatives; Associates; Combination		
Assets/interests at risk		
Business interests; Residence; Office; Property; Reputation/image; Other; Combination		
Nature of threat		
Factual; Imagined; Perceived; Circumstantial; General non-specific; Paranoia		
Type of threat		
Physical (death, injury, kidnap); Embarrassment (media intrusion, eavesdropping, surveillance); Disruptive; Destructive (sabotage); Nuisance; Eavesdropping (snooping, commercial intelligence); Other (intimidation, IT security breaches); Combination		
Commercial intelligence		
Threat	**Primary Targets**	**Sources of Info**
Open market sources; Criminal; Government sponsored	*Research & Development; Tender information; Business world; Financial world*	*Documents and papers; Meetings/eavesdropping; Laptops; Telephone conversations; Employees*
Extent of threat		
Historical incidents (how long, how many, how related, individuals involved, action taken, whether security measures breached (and how), whether there was a build-up); likelihood of escalation; others in similar positions affected		

Motivation
Political (kidnap, ransom, publicity); Criminal (theft, violence, K&R, vandalism); Environmental (activists); Religious; Racial; Cultural; Radical pressure groups; Revenge; Obsession; Grievance; Vendetta; Provoke reaction; Other; Combination
Identified modus operandi/capabilities
Incident reports, etc.
Vulnerability factors
Nationality/race; Religion; Politics; Associations (direct, indirect, sympathetic, supporter); Personal wealth; Social activities; Family routine; Residence location; Routes used; Nature of business; Existing security; Other relevant aspects (e.g. fire/environmental hazards); Presence of other high risk/profile individuals; Mistaken identity; Debts; Legal proceedings (past/present/pending); Indiscretions; Infidelities; Previous history
Principal's health
Age; Fitness; Allergies; Medical history; Family medical history; Chronic conditions; Lifestyle
Principal profile
People: *Family and relatives; Friends; Business associates; Social contacts; Competitors/opponents*
Places: *Born; Educated; Place(s) of abode; Previous addresses; Holidays; Socializing; Sport; Work*
Prejudices: *Religion; Race; Culture; Controversial issues*
Personality: *Poor attitude to security; Arrogant; Brash; Dismissive; Provocative; Boastful; Vain; Violent; Ambitious; Devious; Unscrupulous; Fastidious; Methodical; Mean*
Personal history: *Full name & title; Marital status; Outstanding achievements; Nationalities (previous/current); Languages; Military service; Awards; Qualifications; Positions held; Previous spouse; Children; Medical history; Political history; Convictions*

Private lifestyle:

Family; Relationships; Drinking/eating habits; Gambling; Sporting and leisure activities; Self driven; Work ethic/hours; Public profile; Drug use

Political views:

Influence; Open support; Published opinions and comments; Associations; Donations; Memberships; Political ambition

Perceived threat level and recommendations

Category 1: Client in significant danger. An attack is expected (not "if", but "when").

Recommendations: *CPO; Personal Escort Section; Residential Security Team; Security Advance Party; OST; Armoured vehicle; Full electronic, physical and technical cover*

Category 2: Client in some danger. An attack is possible (not "when", but "if").

Recommendations: *CPO; Personal Escort Section; Selected aspects of Category 1 protection as necessary*

Category 3: Possible chance of threat. Small chance of attack. Client could be a potential target.

Recommendations: *Possible CPO; Routine searches; Surveillance awareness; Security awareness; Personal Escort Section and Residential Security Team as necessary*

NOTE: Both Category 1 and Category 2 involve 24 hour-a-day cover.

Other information/remarks

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS 5454, *Recommendations for the storage and exhibition of archival documents*

BS 7799-1, *Information technology – Security techniques – Code of practice for information security management*

BS 7799-2, *Information technology – Security techniques – Information security management systems – Requirements*

BS 8507-2, *Code of practice for close protection services – Part 2: Operations outside the United Kingdom*[2)]

Other publications

[1] GREAT BRITAIN. The Private Security Industry Act 2001. London: The Stationery Office.

[2] GREAT BRITAIN. The Data Protection Act 1998. London: The Stationery Office.

[3] GREAT BRITAIN. The Disability Discrimination Act 1995 (as amended). London: HMSO.

[4] GREAT BRITAIN. The Human Rights Act 1998. London: The Stationery Office.

[5] GREAT BRITAIN. The Race Relations Act 1976. London: HMSO.

[6] GREAT BRITAIN. The Rehabilitation of Offenders Act 1974. London: HMSO.

[7] GREAT BRITAIN. The Sex Discrimination Act 1975. London: HMSO.

[8] http://www.the-sia.org.uk/NR/rdonlyres/FD8F90B5-5CB0-4F71-BA1D-B9A174319B6A/0/sia_cp_competency.pdf

Websites

http://www.the-sia.org.uk

2) In preparation.

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email bsmusales@bsigroup.com.

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Copyright

Useful Contacts:

Customer Services
Tel: +44 845 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 845 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

bsi.

...making excellence a habit.™