

BS 7858:2012



BSI Standards Publication

Security screening of individuals employed in a security environment – Code of practice

bsi.

...making excellence a habit.
AVA Documents™
Document Sharing Hub

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2012

Published by BSI Standards Limited 2012

ISBN 978 0 580 73505 9

ICS 13.310

The following BSI references relate to the work on this standard:

Committee reference GW/3

Draft for comment 12/30237323 DC

Publication history

First published June 1996

Second edition, March 2004

Third edition, August 2006

Fourth edition, October 2012

Amendments issued since publication

Date	Text affected
------	---------------

Contents

Foreword *ii*

1	Scope	1
2	Terms and definitions	1
3	Risk management	2
4	Security screening process	3
5	Ancillary staff	13
6	Acquisitions and transfers	13
7	Subcontractors	13
8	Individuals employed in security screening	14
9	Records held after cessation of employment	14

Annexes

Annex A (normative) Example forms	16
-----------------------------------	----

Bibliography	27
--------------	----

List of tables

Form 1 – Oral enquiry — Previous employer	17
Form 2 – Oral enquiry – Other than previous employer	18
Form 3 – Request for confirmation of information given orally	19
Form 4 – Verification progress sheet	20
Form 5A – Application form	21
Form 5B – Authorization and compliance	24
Form 6 – Statutory declaration	25
Form 7 – Executive acceptance of risk	26

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 28, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and comes into effect on 1 May 2013. 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.

Supersession

This British Standard supersedes BS 7858:2006+A2:2009, which will be withdrawn on 31 April 2013.

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 requirements are expressed in sentences in which the principal auxiliary verb is "shall".

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

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.

1 Scope

This British Standard gives recommendations for the security screening of individuals to be employed in an environment where the security and/or safety of people, goods and services, personal data or property is a requirement of the employing organization's operations and/or where such security screening is in the public and/or corporate interest.

NOTE 1 "Property" includes intellectual and physical property as well as cash and valuables.

NOTE 2 See Home Affairs Committee First Report: The Private Security Industry Volume 1 [1].

NOTE 3 Some insurers require BS 7858 as a part of the policy conditions and may have additional requirements for screening, e.g. a longer security screening period.

This British Standard applies equally to all individuals in relevant employment (see 2.8), including full-time and part-time employees, sole traders, partnerships, temporary and permanent employees, and to all levels of seniority, including directors. The objective of security screening is to obtain sufficient information to enable organizations to make an informed decision on employing an individual in a security environment.

2 Terms and definitions

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

2.1 ancillary staff

individual(s) involved in ancillary activities such as administration, personnel, building maintenance and cleaning

2.2 conditional employment

period of employment during which security screening is continuing

NOTE Successful completion of security screening is one criterion upon which the decision to grant confirmed employment is based.

2.3 confirmed employment

employment granted upon successful completion of security screening and any additional criteria applied by the organization

2.4 executive

director, partner or sole owner of the organization, or a manager of the organization duly authorized in writing by a director, partner or sole owner of the organization

2.5 individual

person required to be security screened

NOTE An individual might be new to the organization or an existing employee transferring roles within the organization.

2.6 limited security screening

along with information required and preliminary checks, the minimum amount of security screening necessary to be completed satisfactorily before an offer of conditional employment can be made

2.7 organization

company (including sole traders and partnerships), establishment, government or local authority department, or other body employing and/or contracting individuals, including volunteers, in an environment where the security and/or safety of people, goods and services, personal data or property is a significant consideration

2.8 relevant employment

employment which involves, or may involve, the acquisition of, or access to, information, assets or equipment, the improper use of which could involve the organization, any client of the organization, or any third party, in a security risk

NOTE 1 The definition applies to individuals irrespective of whether they are engaged full-time or part-time, on a permanent or temporary basis, and/or employed directly or as subcontractors.

NOTE 2 Further guidance on individuals considered under relevant employment can be found in The Information Commissioners Employment Practices Data Protection Code – Part 1: Recruitment and Selection [2].

2.9 screening controller

individual within an organization, responsible for making sure that the security screening process is being carried out correctly

2.10 screening officer

individual within an organization, engaged in security screening or a third party providing security screening services

2.11 security screening form(s)

suitable form(s) used to gather and record information required to security screen

2.12 security screening period

period of not less than five years immediately prior to the commencement of relevant employment or transfer to relevant employment, or back to the age of 16 if this date is more recent

2.13 subcontractor

company, agency worker(s), individual(s) and temporary worker(s) not directly employed by the organization, contracted to carry out work on behalf of the organization

2.14 wet signature

original signature written on a piece of paper, as opposed to a fax copy or an agreement offered orally or electronically

2.15 writing

legible document (hardcopy document or electronically stored document capable of being printed and/or viewed on screen)

NOTE For verification of identity of signatories to electronic documents, attention is drawn to The Electronic Communications Act 2000 [3].

3 Risk management

The organization should not employ individuals whose career or history indicates that they would be unsuitable for the role, given that such employment might allow opportunities for illicit personal gain, or the possibilities of being compromised, or opportunities for creating any other breaches of security.

NOTE 1 Attention is drawn to UK employment law, commercial insurance cover and the applicable terms and conditions of employment.

The organization should ensure that all individuals employed in security screening (see Clause 8), and those with authority to offer employment, maintain high standards of honesty and integrity in view of the special circumstances of the environment in which they are employed.

Although no system of security screening can provide absolute security, the organization should endeavour to ensure that the integrity of its personnel is established and maintained.

NOTE 2 An integral part of risk management is to provide a structured process for organizations to identify how objectives might be affected. It is used to analyse the risk in terms of consequences and their probabilities before the organization decides what further action is required.

NOTE 3 In some cases, where the verification procedures cannot be completed satisfactorily, employment might be prevented, terminated or employment offer withdrawn. It is emphasized that this is not necessarily an indication of unsuitability; it might simply not have been possible to obtain the required positive evidence.

4 Security screening process

4.1 Overview

The organization should carry out security screening in accordance with this British Standard prior to the engagement of individuals for relevant employment or to their being transferred to relevant employment from other duties.

NOTE 1 For acquisitions and transfers see Clause 6.

NOTE 2 Where labour is subcontracted see Clause 7.

The organization should ensure that employees already in relevant employment are security screened in accordance with this British Standard.

NOTE 3 Attention is drawn to the Data Protection Act 1998 [4] and the Employment Rights Act 1996 [5].

NOTE 4 It is not a provision of this British Standard that employees already screened to previous editions of this standard are re-screened, provided evidence of previous screening can be clearly demonstrated.

The full security screening process should be carried out in accordance with this standard, regardless of an individual's previous employment, even if that employment was in a security environment.

NOTE 5 Attention is drawn to the Rehabilitation of Offenders Act 1974 [6].

4.2 Administration

The screening controller should ensure that screening data is held confidentially and stored securely to prevent unauthorized access and alteration.

NOTE 1 Attention is drawn to the Data Protection Act 1998 [4] which requires organizations that are Data Controllers to notify the Information Commissioner's Office of the processing that is taking place.

NOTE 2 With regard to the storage of electronic data, attention is drawn to the following standards; BIP 0008-1 and BS ISO/IEC 27001 (BS 7799-2) and BS ISO/IEC 27002 (BS 7799-1).

The organization's security screening working practices should be regularly reviewed and updated if necessary, and should deal with such matters as clearing desks, locking filing cabinets, etc. at the end of the working day; security shredding and disposing of waste paper (including spoiled documents, etc.); the control of access to computers and data storage media, recordings of telephone conversations, etc.

NOTE 3 Attention is drawn to the Information Commissioner's Employment Practice Code [2], and the need to comply with any obligations in the Information Commissioner's Code.

Organizations should maintain the following in electronic or paper format:

- a) a separate file for each individual subjected to security screening. The files of all individuals currently employed but still subject to completion of screening should be identified separately from other employee files; and
- b) verification progress sheets (or equivalent) for each individual subjected to security screening.

Where applicable, records should clearly indicate that an individual is conditionally employed but still subject to completion of screening. Records should show prominently the dates on which such employment commenced and is to cease if screening is not completed within 12 or 16 weeks after the date of commencement, dependent on the security screening period.

The screening file should be retained during employment (see also Clause 9).

4.3 Provision of information

4.3.1 General

Written evidence should be obtained to see if there is anything in the individual's background which would reflect adversely upon their suitability for the proposed employment (see Clause 3).

NOTE When obtaining written references, it is important to be sure that the source is genuine. If considered necessary, extra checks can be made to verify the validity of facsimile numbers, postal and email addresses.

4.3.2 Authorizations

The security screening form should state that information is gathered to facilitate security screening in accordance with BS 7858, in order to determine whether individuals are suitable to be employed in a security environment.

The organization should make the individual aware at their interview or application, whichever is appropriate, that, with the individual's written permission, the organization is authorized to obtain the following in accordance with relevant legislation:

- a) *background career/history checks.* if permission to contact a current employer is withheld until an offer of employment is made, the individual should be informed that a condition of the offer of employment is that the offer can be withdrawn if the security screening is not concluded satisfactorily. The period of current employment should initially be verified by a personal reference and/or documents which substantiate employment;
- b) *a search of public record information.* e.g. County Court Judgments, bankruptcies, financial sanctions ¹⁾ and proof of identity and proof of address; and
- c) *a criminality check:* see 4.7j).

¹⁾ See http://www.hm-treasury.gov.uk/fin_sanctions_index.htm.

4.3.3 Information required

The organization should request the following information at the appropriate point of the screening process.

- a) The individual's personal details including:
 - 1) full name, including forename(s) and surname/family name(s);
 - 2) other and/or previous forename(s) and surname/family name(s) used during the security screening period;
 - 3) aliases, i.e. any name(s) used in addition to current or previous name(s) during the security screening period;
 - 4) full address history, including "from" and "to" dates, for the past five years;
 - 5) date of birth;
 - 6) National Insurance number;
 - 7) evidence of right to work in the UK ²⁾;
 - 8) SIA licence number and expiry date (if held).
- b) Details of the individual's education, employment, periods of self-employment (see 4.7), unemployment and gaps in employment (including career breaks, etc.) throughout the security screening period.

NOTE 1 If an individual does not want the organization to contact their current employer until an offer is made see 4.3.2a).

Organizations should extend the security screening period (see 2.12) to account for:

- 1) contractual or legislative considerations; and/or
 - 2) specific industry standards.
- c) The name of one referee, with personal knowledge of the individual, from whom a written character reference should be obtained.

The security screening form(s) should state that the individual(s) providing character references will be asked to confirm the nature of their relationship with the individual being security screened, and that they have known the individual for a minimum of two years immediately prior to the start of security screening. The security screening form(s) should also state that character references should not be obtained from previous employers, relatives (by blood or by marriage) and/or persons residing at the same address as the individual.
 - d) Details of all cautions or convictions for criminal offences, including motoring offences and pending actions, subject to the provisions of the Rehabilitation of Offenders Act 1974 [6].
 - e) Details of all bankruptcy proceedings and court judgments (including satisfied), financial judgments in the civil court made against the individual and individual voluntary arrangements with creditors from the previous six years.
 - f) An acknowledgement that misrepresentation, or failure to disclose material facts, either during application or throughout employment may constitute grounds for withdrawal of an employment offer or termination of employment and/or legal action.

²⁾ See www.direct.gov.uk/en/Employment/Understandingyourworkstatus and www.ukba.homeoffice.gov.uk/visas-immigration/working.

- g) A statement, in writing, authorizing the organization to approach current and former employers, government departments, individuals providing character references, etc. for verification of a continuous record of their career and history.

NOTE 2 See also 4.3.2.

NOTE 3 Authorization may be in the form of either a wet signature or electronic confirmation. Some organizations might only accept a wet signature.

NOTE 4 An example of the text that can be used is given in Annex A, Form 5B, which can be used as a separate form or as part of the application form.

- h) A declaration signed by the individual which acknowledges that employment is subject to satisfactory screening, that the individual consents to being screened and will provide information as required, that information provided is correct, and that any false statements or omissions could lead to termination of employment (a suitable example is provided in Annex A, Form 5B).

4.3.4 Interview

Organizations should interview the individual before any offer of employment is made.

NOTE It is preferable that interviews are carried out with the individual physically present. However, if a physical meeting is not possible at the interview stage then attention is drawn to 4.4c).

4.4 Preliminary checks

Preliminary checks should, as a minimum, include the following for each individual being security screened:

- a) Establishment of a screening file in accordance with 4.2a);
- b) All information requested in accordance with 4.3.3 has been supplied (e.g. through a fully completed application form) and a full review of the information provided to confirm that the individual is likely to complete security screening;

NOTE 1 Information can be supplied in either paper or electronic format. However, certain documentation such as documentation for confirming identity [see 4.4c)] and current address of residence [see 4.4d)] needs to be hardcopy originals.

NOTE 2 In some circumstances an original wet signature on the signed authorization to approach third parties will be required.

- c) Confirmation of identity including verification of documents.

NOTE 3 Acceptable documents are as in accordance with Group A and Group B of the SIA identity verification criteria ³⁾.

Wherever possible, the supporting documentation should be photographic i.e. passport or photo identification drivers licence. Verification should include visual inspection of original documents and retention of a copy. The visual inspection should compare details within the document against the physically present individual and a check for signs of tampering or alteration.

Organizations should also carry out verification checks according to the following circumstances:

- 1) *Individual holding a valid and current SIA licence* - The organization

³⁾ <http://www.sia.homeoffice.gov.uk/Pages/licensing-id-checklist.aspx>

should see the original licence and verify it against the public register of licence holders. The document details should be cross-checked against other information provided by the individual.

NOTE 4 As part of the SIA licence application process, identity documents are checked.

A copy of the public register search result should be retained on file.

NOTE 5 Further verification of identity documents may be carried out at the discretion of the organization using electronic means.

- 2) *Individual not holding a valid and current SIA licence* - The organization should be able to demonstrate that they have taken necessary steps to confirm the identity of the individual.

NOTE 6 Additional electronic verification may be undertaken for example a passport can have its Machine Readable Zone (MRZ) verified by using a passport scanner or using an online service or using a third party organization. Third parties may also be able to carry out checks on other types of documents to provide further verification where required by the organization.

A copy of the document(s) produced should be retained in the screening file together with details of who examined and copied the original document and evidence of any additional electronic check(s). Details within the document(s) should be cross-checked against other information provided by the individual.

NOTE 7 Examples of authentic documents, such as an SIA licence, passport and visa stamps, can be found on Government department web sites. For SIA licensing and details of acceptable identity documents, refer to www.sia.homeoffice.gov.uk.

NOTE 8 Attention is drawn to the Immigration, Asylum and Nationality Act 2006 [7], Accession (immigration and worker registration) Regulations 2011 [8], Sections 15 to 26 of The Immigration (restrictions on employment) Order 2007 [9] and The Immigration (employment of adults subject to immigration control) (maximum penalty) Order 2008 [10].

NOTE 9 Information relating to the prevention of illegal working can be found on the Home Office UK Border Agency website www.ukba.homeoffice.gov.uk.

- d) Confirmation of current address of residence: the documents that should be presented are listed on the SIA website (<http://www.sia.homeoffice.gov.uk/>) and conform to the SIA requirements for licensing.

Copies of the documents should be retained in the screening file, with details of who examined and copied the original document.

Any documents presented to establish proof of address of residence should be checked for authenticity.

- e) The individual's public financial information: the organization should establish these details by direct reference through a credit reference agency or its agent. The organization should include the following official public record information in the search:
- 1) confirmation that the individual is listed on the electoral roll;
 - 2) if not listed on the electoral roll then confirmation that the individual is known at the current address of residence;
 - 3) linked postal address for the previous five years should also be searched to ensure no adverse information is listed;
 - 4) county court judgments (CCJs) including IVAs;
 - 5) bankruptcy orders;