BS 8549:2016

BSI Standards Publication

Security consultancy – Code of practice

bsi.

Publishing and copyright information

Published by BSI Standards Limited 2016

ISBN 978 0 580 90715 9

ICS 03.080.20; 13.310

The following BSI references relate to the work on this document:
Committee reference GW/3/-/26
Draft for comment 16/30326057 DC

Publication history

First published, November 2006
Second (present) edition, August 2016

Amendments issued since publication

Date	Text affected

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 12, 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 came into effect on 31 August 2016. It was prepared by Subcommittee GW/3/-/26, *Security Consultancy*, under the authority of Technical Committee GW/3, *Private Security Management & Services*. A list of organizations represented on this committee can be obtained on request to its secretary.

Supersession

This British Standard supersedes BS 8549:2006, which is withdrawn.

Information about this document

This is a full revision of the standard, and introduces the following principal changes:

- new recommendations with regard to:
    - data backup;
    - implementation, verification and testing;
- the addition of Annex A, Example code of conduct.

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.

Requirements in this standard are drafted in accordance with *Rules for the structure and drafting of UK standards*, subclause **J.1.1**, which states, "Requirements should be expressed using wording such as: 'When tested as described in Annex A, the product shall ...'". This means that only those products that are capable of passing the specified test will be deemed to conform to this standard.

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 management, resourcing and operation for the provision of contracted security consultancy services.

NOTE 1 The services offered by a security consultancy might include, but are not limited to:

a) assessing and identifying security risks to the customer's organization;

b) advising on the adequacy of resilience, existing procedures, defences and processes – and outlining areas of possible improvement;

c) development and maintenance of policies and plans etc.;

d) strategic planning;

e) crisis management;

f) budget management;

g) providing training to the customer's members of staff;

h) pre-employment screening;

i) workplace investigation, see also BS 102000;

j) asset and lone worker tracking;

k) acting as an expert witness in court cases (civil and criminal); and

l) compliance management.

This British Standard also assists procurers wishing to contract such services to ensure the service fits the end user requirements and risk profile.

NOTE 2 Security consultancy services can be provided by any legally defined trading style, e.g. self-employed, a sole trader, a partnership, a limited liability partnership or an incorporated company.

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*

3 Terms and definitions

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

3.1 customer
individual(s), public or corporate body retaining the services of a consultancy

3.2 deliverable
measurable and tangible outcome of the project as agreed with the customer

3.3 milestone
checkpoint within the life of the project identifying when one or multiple groups of activities have been completed

3.4 operational centre
centre where activities of a business, organization, etc. are administrated and take place

NOTE This can be physical or virtual.

3.5 scope of work
document detailing specific contractual services

3.6 security consultancy
individual or organization that is the prime provider of contracted services

NOTE This definition also applies to a security consultant acting in a self-employed capacity, a sole trader, a partnership, limited liability partnership or an incorporated company.

3.7 security consultant
individual giving advice with regard to:

a) security policies, processes and procedures in relation to any risk to property, people or other tangible/intangible assets; or

b) the use of any services involving the activities of security operatives

3.8 security operative
individual or company that performs activities relating to the provision of security services

3.9 supplier
individual or company (and the persons employed, including all levels of subcontractor, by that individual or company) that provides the consultancy with information, equipment and/or labour which is used in providing the service to the customer

3.10 technical expert
individual who provides specific knowledge or expertise for the fulfilment of the contract

4 The consultancy

4.1 Code of conduct

The consultancy should produce a code of conduct which sets out its approach to services, by which it abides and which is available to the customer.

The code of conduct should cover, but not be limited to, the consultancy's values, obligations, duties, practices and compliance.

In particular, the code of conduct should include:

a) responsibility and accountability;

b) honesty and integrity;

c) conflicts of interest;

d) compliance with the law;

e) authority, respect and courtesy;

f) equality;

g) confidentiality;

h) general conduct; and

i) challenging and reporting improper conduct.

NOTE 1 An example code of conduct is given in Annex A.

NOTE 2 Attention is drawn to the Data Protection Act 1998 [1].

4.2 Structure

The consultancy should have a clearly defined management structure showing control and accountability at each level of operation.

Details of the consultancy owner should be made available. Any relevant unspent criminal convictions, business failures or liquidations, or undischarged bankruptcy of the owner should be disclosed on request.

NOTE Attention is drawn to the Rehabilitation of Offenders Act 1974, as amended [2], whose provisions, if applicable, govern such disclosure.

Details of the consultant(s) responsible for the delivery of the contracted services should be established and their curriculum vitae and details of experience made available to customers on request.

4.3 Subcontractors

Where the customer permits the use of subcontractors, they should be required to comply with the consultancy's code of conduct, see **4.1**.

4.4 Finances

The consultancy should act with financial probity and have in place the resources and financial controls to provide the contracted services.

Supplier and subcontractor fees should be paid promptly and within contracted timescales.

4.5 Insurance

The consultancy should possess all necessary insurance cover commensurate with the contracted services provided and the number of persons employed, e.g. professional indemnity, public liability, efficacy liability, employer's liability, which should be made available on request.

4.6 Administrative office and/or operational centre

The consultancy 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 are held in accordance with **4.7**.

4.7 Documented information

Separate records (hardcopy or electronic) maintained for each customer, employee, sub-contractor and supplier should be held in an accessible and secure manner and retained for an agreed period after which they should be securely destroyed. Where no requirement for the period of retention of documents exists, records should be kept for a minimum of 12 months from cessation of contract, after which they should be securely destroyed. Amended and/or updated records should be identifiable by date and clearly distinguishable from previous versions.

NOTE 1 Attention is drawn to the Data Protection Act 1998 [1] and associated guidance note.

NOTE 2 Attention is also drawn to the fact that certain records have a statutory minimum retention period and/or are covered by other Acts.

4.8 Information backup

Backup copies of information, software and system images should be taken and regularly tested in accordance with company policy.

Copies should be securely stored separately in a different location or, if not possible, in a different fire zone within the same location.

NOTE Attention is drawn to BS ISO/IEC 27001.

4.9 Complaints management

The consultancy should operate a complaints management system.

NOTE Further guidance on complaints management is given in BS ISO 10002.

5 Personnel

*COMMENTARY ON CLAUSE **5***

A nationally recognized body or agency could undertake the personnel processes and validations outlined in this clause on behalf of the consultancy.

5.1 Selection and security screening

All personnel who have access to information and/or property of the customer or the consultancy should be screened in accordance with BS 7858 and be bound by an agreement to keep confidential such information indefinitely, unless otherwise authorized in writing.

NOTE Higher levels of security screening might be required as appropriate to the contracted services.

The consultancy service provider should ensure that all personnel are obliged to declare immediately any changes to the information obtained during the selection process.

5.2 Disciplinary code

All personnel should be instructed that the following (including the aiding and abetting of others) could constitute a breach of the terms and conditions of engagement:

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 organization or customer, either past or present, without permission;

f) soliciting or receipt of gratuities or other consideration from any person;

g) failure to account for keys, money, information or property 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 organization, customer or a fellow employee;

j) use of uniform, 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 and/or motoring offence;

2) indictment for any offence;

3) police caution;

4) legal summons;

5) refusal, suspension or withdrawal (revocation) of a licence.

NOTE 1 An example of such a licence would be a Security Industry Authority (SIA) licence. For definitions see the SIA website, http://www.sia.homeoffice.gov.uk/Pages/home.aspx.

m) permitting unauthorized access to a customer's premises;

n) carrying of equipment not issued as essential to an employee's duties, or use of a customer's equipment or facilities without permission; and

o) not maintaining agreed standards of appearance and deportment whilst at work.

NOTE 2 This list is not exhaustive and does not necessarily include all actions within a company policy that could or could not constitute criminal offences.

5.3 Identification

Persons who have been screened in accordance with **5.1** should be issued with an identity card incorporating, as a minimum, the following information:

a) the name, address and telephone number of the consultancy;

b) the name, job title and signature of the holder;

c) the expiry date of the card (not more than three years from the date of issue); and

d) a current photograph of the holder.

Identity cards should be presented to the customer on request.

Old or out of date identity cards should be formally withdrawn from persons renewing their cards. Cards should be returned when an employee leaves the employment of the consultancy, and destroyed in a secure manner.

A record of identity cards issued should be maintained. This record should also indicate the status and location of withdrawn cards, e.g. whether they have been destroyed or lost, or where they are held by the employee/organization.

5.4 Training

5.4.1 General

The consultancy should have a clearly defined and documented training policy and should ensure that the training outlined in **5.4.2**, **5.4.3** and **5.4.4** is given as a minimum.

5.4.2 Induction

The consultancy should provide induction training in matters relating to its conditions of employment, structure and procedures for all employees. This induction training should be additional to the competence recommendations in **5.4.3**.

5.4.3 Competence

Security consultants should be able to demonstrate that they have undergone training on the main aspects of security consultancy which could include, where relevant:

a) threat and risk assessment;

b) security audits, surveys and reviews;

c) security strategy, management, policy and procedures;

d) crisis management and business continuity planning;

e) physical security;

f) electronic security systems;

g) manned guarding;

h) IT and information security;

i) health and safety;

j) construction design and management regulations (CDM);

k) fire safety;

l) investigative practice;

m) human rights;

n) civil and criminal law;

o) data protection; and

p) disability issues.

*NOTE Attention is drawn to the recommendations in **5.4.5**.*

5.4.4 Continuing professional development (CPD)

The consultancy should ensure that each security consultant undertakes a minimum of 20 hours of CPD per annum.

NOTE CPD can consist of relevant training undertaken in the classroom, e-learning, research, exhibitions, conferences or any other recognized form of CPD.

5.4.5 Records

All CPD and training undertaken should be recorded and endorsed by the trainer or other authorized person.

Evidence of appropriate CPD should be made available on request.

Training records should be reviewed annually by the consultancy, to ensure that appropriate training has been provided.

NOTE Individuals who belong to a recognized professional body could have their CPD verified by that organization.

5.5 Suppliers

5.5.1 Subcontractors

The consultancy should obtain the customer's documented agreement on the conditions to subcontract all or part of the services, i.e. to another security consultant or technical expert.

5.5.2 Subcontractor personnel

The consultancy should satisfy itself that those subcontractor's personnel who have access to a customer's site and/or confidential records:

a) meet the recommendations for professional integrity in **4.1**;

b) are security screened in accordance with **5.1**;

c) are competent to undertake the work involved;

d) are insured in accordance with **4.5**;

e) have signed a confidentiality agreement relating to the disclosure of the customer's and the consultancy's confidential information and/or material;

f) agree to report immediately to the consultancy any contravention (both alleged and actual) of the law; and

g) have received, prior to engagement, appropriate induction training relevant to the contracted services, including the code of conduct.

Evidence of a) to g) should be retained by the consultancy and reviewed, as a minimum, annually.

6 Consultancy service

6.1 Sale of services

6.1.1 Customer information

The consultancy should provide potential customers with basic information of name, address, directors, principals and people with significant control of the consultancy.

NOTE This information could take the form of a brochure or be made available on a website.

If requested by a potential customer, the consultancy should supply the following additional information:

a) terms and conditions of trading;

b) the type and extent of insurance cover;

c) reference sources of work carried out by the consultancy;

d) details of proposed personnel; and

e) annual accounts.

6.1.2 Scope of work

Prior to commencement of any security consultancy service, the consultancy should agree with the customer the scope and extent of the work required. This should be clearly defined, show deliverables and milestones and be presented to the customer in documented form as part of the proposal.

The work should only be undertaken if, after consultation with the customer, it is the opinion of the consultancy and the security consultant(s) involved that:

a) there is sufficient and appropriate information about the scope of work; and

b) the consultancy is competent to undertake the work.

6.1.3 Proposal

A written proposal should be provided by the consultancy. If accepted by the customer, it should form part of the contract. The proposal document should include:

a) the terms and conditions under which the work would be carried out;

b) the costing for the service, and the arrangements for payment;

c) the contract period;

d) reference to the scope of work including deliverables and milestones, if relevant;

e) the obligation of the customer to identify and consult with the consultancy on any specific health and safety requirements that apply, or are likely to apply, during the period of the contract;

f) any issues regarding intellectual property rights;

g) a statement including, as a minimum, the full name and previous relevant experience and qualifications of the security consultant(s) who might be involved in any proposed consultancy service and their relationship with the consultancy; and

h) provision for changes in the scope of work that result in delays in carrying out the work due to circumstances beyond the control of the consultancy.

6.1.4 Contracts

The customer should be asked to agree to provide either:

a) formal confirmation that they have read, understood and accepted the proposal and terms and conditions; or

b) a contract document referring to the proposal and terms and conditions.

The contract should be agreed and exchanged before work commences.

6.2 Delivery of service

6.2.1 Contracted services

The contracted services should be in accordance with the agreed proposal.

*NOTE The scope of work identifies the exact areas of work, see **6.1.2**.*

6.2.2 Assessment

A documented assessment for the delivery of contracted services should be based on an evidence-based approach and might include:

a) existing controls;

b) interviews, e.g. key stakeholders;

c) examination of existing issues, e.g. current security systems and condition;

d) documents, e.g. specifications, policies and procedures;

e) observations of locations, e.g. physical layout;

f) activities and conditions, e.g. people and the environment; and

g) existing results of measurements and a range of tests or other means within the scope of the assessment, e.g. risk assessments, security records.

NOTE The issues identified by the documented assessment could be addressed by implementing or amending appropriate governance practices and/or control measures.

6.3 Reporting

The consultancy should proactively communicate with the customer to ensure that key messages through the implementation phase of a project are passed on. These should not be limited to just positive information but should also include any issues that might adversely impact on the successful delivery of the consultancy project particularly if budgets or the completion date might be affected.

On completion of the contracted scope of work, the consultancy should provide a report of their findings.

NOTE 1 This can take the form of a written report or verbal briefing dependent on the terms of the contract.

EXAMPLE

The report could cover, but not be limited to, the following.

a) Customer.

b) Location.

c) Date of work.

d) Scope of work.

e) Executive summary.

f) Methodology.

g) Observations.

h) Recommendations (could include guidance on cost and timescales).

i) Conclusions.

Observations and recommendations contained in the report should be based on policies, practices, procedures or requirements against which the consultancy compares collected evidence about the subject matter.

NOTE 2 Requirements might include, but are not limited to, standards, guidelines, specified requirements and legislative or regulatory requirements.

7 Implementation, verification and testing

7.1 Implementation

The agreement reached between the consultancy and the customer should include, where required (but not necessarily be limited to):

a) methodology;

b) deliverables;

c) milestones; and

d) reporting (see **6.3**).

7.2 Verification and testing

NOTE 1 Verification is the process by which the consultancy achieves formalized acceptance, usually from the customer, of the completed project deliverables.

The consultancy should ensure that within the agreement there are suitable and sufficient measures and arrangements in place by which verification can be confirmed.

NOTE 2 These might include (but not necessarily be limited to):

a) Meetings. Regular meetings where an agreed agenda is discussed and minutes taken and distributed to all attendees (and those who are involved in the project).

b) Formal sign off and acceptance of works. This might occur after individual key milestone dates or on the implementation of agreed deliverables or only on completion of the consultancy project. This could be particularly important if there is a staged payment plan in place that is triggered by client acceptance of deliverables.

c) Third party sign off. In the event that the consultancy deliverables require independent, third-party verification, testing and approval before the project might be considered as complete.

The consultancy should satisfy itself that it has suitably robust sign-off capability within the overall project plan to ensure that any key deliverables can be approved.

Annex A (informative) Example code of conduct

A.1 Responsibility and accountability

Our consultants are personally responsible and accountable for their actions, as are our employees and other persons paid to assist an investigation.

A.2 Honesty and integrity

Our consultants act with honesty and integrity, and do not compromise their position, that of the service provider or any of their customers.

A.3 Conflict of interest

Where our consultants have a personal or conflicting interest in any matter in which they are involved they disclose that interest, if they know it to be in conflict with the interests of their customers.

A.4 Compliance with the law

Our consultants obey the law and refrain from carrying out any act that they know, or ought to know, is unlawful or contrary to the service provider's policy.

A.5 Authority, respect and courtesy

Our consultants respect the rights of all individuals and do not abuse their position.

A.6 Equality

Our consultants act with fairness and impartiality. They do not discriminate on the grounds of sex, race, colour, language, religion or belief, political or other opinion, national or social origin, association with a national minority, disability, age, sexual orientation, property, birth or other status.

A.7 Confidentiality

Our consultants treat with respect any information with which they are entrusted during the course of business, and access or disclose it only for the purposes for which it is intended.

A.8 General conduct

Our consultants act in a professional manner. They do not behave in a manner which brings, or is likely to bring, discredit upon themselves, the service provider or any of their customers, or act in a way that undermines or is likely to undermine confidence in themselves, the service provider or that of any of their customers.

A.9 Challenging and reporting improper conduct

Our consultants challenge and, when appropriate, take action or report breaches of this code and the improper conduct of colleagues.

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 102000, *Code of practice for the provision of investigative services*

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

BS ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

Other publications

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

[2] GREAT BRITAIN. Rehabilitation of Offenders Act 1974. London: The Stationery Office.

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.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing 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 subscriptions@bsigroup.com.

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.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 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 Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.