BS 10501:2014

BSI Standards Publication

Guide to implementing procurement fraud controls

bsi.

...making excellence a habit.™

Publishing and copyright information

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

© The British Standards Institution 2014

Published by BSI Standards Limited 2014

ISBN 978 0 580 82874 4

ICS 03.100.10; 13.310

The following BSI references relate to the work on this document:
Committee reference G/2
Draft for comment 13/30282472 DC

Publication history

First published March 2014

Amendments issued since publication

Date	Text affected

BSI acknowledges the contribution of CIPS in the initiation and development of this standard.

The Chartered Institute of Purchasing & Supply (CIPS) is the world's largest procurement and supply professional organization. It is the worldwide centre of excellence on purchasing and supply management issues. CIPS has a global community of over 100,000 in 150 different countries, including senior business people, high-ranking civil servants and leading academics. The activities of purchasing and supply chain professionals have a major impact on the profitability and efficiency of all types of organization and CIPS offers corporate solutions packages to improve business profitability.

www.cips.org; @CIPSNews

Contents

Summary of pages

This document comprises a front cover, an inside front cover, pages i to ii, pages 1 to 24, 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 March 2014. It was prepared by Technical Committee G/2, *Anti procurement fraud*. A list of organizations represented on this committee can be obtained on request to its secretary.

Use of this document

As a guide, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any 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.

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.

Introduction

Procurement is defined by this British Standard as the "process of acquiring goods, works and/or services, covering both the acquisition from third parties and in-house providers, and spanning the whole life cycle from identification of needs through to the end of a services contract or the end of the useful life of an asset".

This definition is important as it is where the process of identifying the risk of procurement fraud begins. The possibility of procurement fraud needs to be considered from the very beginning of the procurement activity. This includes the method by which the goods, works or services are going to be procured, such as written quotations, single/sole sourced or through a competitive tender.

It is best practice to design out the possibility of procurement fraud at the earliest opportunity and this British Standard provides guidance on mitigating a range of fraud risks.

1 Scope

1.1 This British Standard gives guidance on mitigating and actively managing the following procurement fraud risks:

a) procurement fraud committed against the organization by its personnel or others acting on its behalf or for its benefit;

b) procurement fraud committed against the organization by another organization or individuals with the assistance of its personnel or others acting on its behalf or for its benefit;

c) procurement fraud committed against the organization by another organization or their personnel;

d) procurement fraud committed against the organization by other organizations or their personnel acting on their behalf, e.g. fraud conspiracy, bid rigging, anti-competitive activity.

1.2 This British Standard is applicable only to procurement fraud, specifically fraud offences committed in the procurement life cycle. It is not applicable to other criminal offences, such as anti-trust/competition and money laundering offences, although an organization may choose to extend the scope of its procurement fraud controls to include these other offences.

NOTE Many countries' laws do not define procurement fraud or define fraud in different ways. This standard does not provide its own definition of fraud, but identifies the following specific fraud types where it is committed: false representation, failing to disclose information when there is a legal duty and/or contractual obligation to do so and abuse of position.

1.3 This British Standard is applicable to all types and sizes of organizations (including small and medium enterprises) in all sectors (including the public and private sectors, and the charity and voluntary sectors).

2 Terms and definitions

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

2.1 compliance manager
person responsible for ensuring that the organization's systems of control are operating adequately, including the effective management of procurement fraud risk

NOTE The role of the compliance manager might be full-time or might be performed by a member of staff in addition to their regular role.

2.2 conflict of interest
situation where outside business, family or personal connections could interfere with the judgement of personnel in carrying out their duties for the organization

[SOURCE: BS 10500:2011, modified]

2.3 framework agreement
agreement with suppliers that sets out the terms and conditions governing contracts that can be awarded during the life of the agreement and that might relate to price, quality and quantity under which individual contracts can be made

2.4 information security
preservation of confidentiality, integrity and availability of information, including the protection of information and information systems against unauthorized access or modification of information, whether in storage, processing or transit, and against denial of service to authorized users

NOTE Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security.

2.5 internal audit
systematic, independent and documented process for obtaining evidence and evaluating it objectively in order to determine the extent to which procurement fraud requirements are fulfilled

2.6 organization
corporation, company, firm, partnership, enterprise, authority or institution, or part or combination thereof, whether incorporated or not, public, private or voluntary

[SOURCE: BS 10500:2011, modified]

2.7 personnel
organization's directors, officers, employees, agents and temporary and outsourced staff or workers, paid and unpaid

[SOURCE: BS 10500:2011, modified]

2.8 procure-to-pay
process of acquiring and managing goods, works and/or services needed for manufacturing a product or providing a service, involving the transactional flow of data that are sent to a supplier and the data concerning the fulfilment of the order and payment for the goods, works and/or services

2.9 procurement
process of acquiring goods, works and/or services, covering both the acquisition from third parties and in-house providers and spanning the whole life cycle from identification of needs through to the end of a services contract or the end of the useful life of an asset

2.10 procurement fraud
fraudulent act committed against an organization's procurement process that might involve fraud by false representation, failure to disclose information when there is a legal duty and/or contractual obligation to do so, abuse of position, or associated offences

NOTE A list of the various forms of procurement fraud is given in Annex A.

2.11 procurement fraud control
measure intended to help the organization:

a) identify the risk of procurement fraud;

b) mitigate procurement fraud;

c) detect, report and respond to an allegation or suspicion of procurement fraud; and

d) monitor, review and implement control measures

NOTE Such a measure might be independent or be part of the overall fraud management controls.

2.12 procurement life cycle
phases of the procurement process, from identification of needs through to the end of a services contract or the end of the useful life of an asset

NOTE The procurement process involves options appraisal and the critical "make or buy" decision.

2.13 procurement fraud policy
document that:

a) prohibits procurement fraud; and

b) requires reasonable and proportionate measures to be taken to:

1) mitigate procurement fraud;

2) detect, investigate, report and respond to (e.g. initiate procurement fraud response plan) any procurement fraud that occurs

2.14 purchasing
process of buying materials and services of the required quality, in the correct quantity, delivered to the right place at the right time, from a legitimate source, at an appropriate price

2.15 supplier
organization that provides materials, components, goods, works or services for another organization

2.16 supply chain
movement of materials (or services) as they flow from their source or supplier to the end customer

NOTE 1 A supply chain is made up of the people, activities, information and resources involved in moving a product (or service) from suppliers to customers. Understanding who and what is involved in the supply chain process (which might include a number of tiers) is an essential part of the procurement process.

NOTE 2 An international supply chain organization may be involved in various processes, including manufacturing, processing, loading/unloading, transportation (across international borders), customer service, demand planning, supply planning and supply chain management.

2.17 top management
person or group of people who directs and controls an organization at the highest level

[SOURCE: BS EN ISO 9000:2005]

3 Planning

3.1 General

The organization should plan for the adoption of a procurement fraud policy and the implementation of procurement fraud controls by ensuring that the following steps are taken:

a) allocating responsibility for planning to personnel of appropriate seniority;

b) appointing appropriately qualified personnel to conduct a risk assessment to identify what activities or other aspects of the organization's business have procurement fraud risks;

c) assessing in what manner and to what extent the procurement fraud controls should be implemented by the organization, taking into account the factors in **4.1**;

d) writing the procurement fraud policy;

e) designing or modifying the necessary policies, procedures and controls, and ensuring that they are reviewed at agreed intervals;

f) determining the necessary resources (including funding, personnel, equipment and materials) needed to implement the procurement fraud controls;

g) preparing an implementation timetable with clearly identified responsibilities.

3.2 Assessment of risk

3.2.1 The organization should implement procedures to enable it to assess:

a) the risk of procurement fraud in relation to its existing and proposed procurement and supply chain activities;

b) whether its policies, procedures and controls are adequate to mitigate those risks in line with the organization's risk appetite.

3.2.2 The timing and frequency of risk assessments should be defined by the organization.

3.2.3 As part of its risk assessment process, the organization should conduct due diligence on business suppliers in accordance with **4.12**.

3.2.4 In considering the controls necessary to mitigate risk, there should be adequate review of risk areas within the purchasing process, including:

a) business requirement, i.e. identification of needs;

b) product and/or services specification;

c) assessment of pre-qualification and tender submissions and selection;

d) tender selection and contract award;

e) review of the make or buy decision;

f) ongoing supplier relationship management;

g) asset protection.

3.2.5 When carrying out fraud checks within the procure-to-pay process, the following should be considered.

a) Does the requisition match the purchase order?

b) Is it the same person authorizing both activities? Would segregation of duties be appropriate?

c) Does the purchase order match the requirement in the contract?

d) Does the purchase order match the delivery note?

e) Is there a delivery note to evidence the delivery of the goods, works or services?

f) Are all signatures on the delivery note clearly visible and identifiable to a particular person?

g) Is there signed evidence to demonstrate the services have been completed?

3.2.6 Performance bonuses, performance targets and other incentivizing elements of remuneration should be reviewed to ensure that there are reasonable safeguards to prevent these from encouraging bribery.

3.2.7 Procurement fraud risks should be documented in the risk register and reported to the audit committee. An overview of controls in place and their effectiveness, including near misses for fraudulent activity, should be reported to the audit committee on a predetermined basis.

4 Procurement fraud controls

4.1 Scope of the controls

The controls to be implemented by the organization should be reasonable and proportionate, taking into consideration the nature and extent of the procurement fraud risks that the organization faces and the:

a) size of the organization;

b) countries and sectors in which the organization operates;

c) nature, scale and complexity of the organization's commercial activities and supply chain;

d) organization's existing suppliers.

4.2 Controls

4.2.1 Procurement controls

The organization should implement procurement and other controls to ensure that it can purchase materials and services of the required quality, in the correct quantity, delivered to the right place at the right time, from a legitimate source, at an appropriate price.

4.2.2 Procurement fraud controls

The organization should implement procurement fraud controls that mitigate the risk of the organization, its personnel or others acting on its behalf committing, or being the victim of, procurement fraud.

4.2.3 Bribery controls

Bribery can be part of a procurement fraud conspiracy or facilitate the act of fraud. The organization should implement procurement and other controls which mitigate the risk of the organization, its personnel or others acting on its behalf committing bribery.

NOTE BS 10500 specifies requirements for an anti-bribery management system. Attention is drawn to the corporate liability issues that apply to UK associated business under Section 7 of the Bribery Act 2010 [1] and the potential for acts within an organization's supply chain to confer that liability by association.

4.2.4 Financial controls

4.2.4.1 The organization should implement financial controls that mitigate the risk of the organization, its personnel or its suppliers committing procurement fraud.

4.2.4.2 The organization should maintain records that accurately document all financial transactions.

4.2.4.3 The organization should implement a process for reviewing any agreements to deter informal contract variations.

4.2.5 Quality controls

The organization should implement quality controls, including:

a) mitigating risk to the organization, or any of its personnel, from a supplier or other associated person's use of inferior or substituted goods, works or services for the purpose of committing fraud;

b) mitigating risk by ensuring supplier compliance with regulation and legislation, including health and safety requirements and licensing provisions;

c) monitoring suppliers' compliance with quality assurance requirements, which might indicate the provision of poor quality of goods, works or services or product substitution;

d) maintaining auditable records that accurately document quality control.

4.3 Communicating policy and programme

4.3.1 Top management should make a statement that:

a) the organization has adopted a policy that supports and incorporates the procurement fraud controls;

b) the organization is implementing procurement fraud controls to give effect to this policy;

c) top management supports the policy and the implementation of procurement fraud controls.

NOTE This statement is likely to be made by the Chairperson, Chief Executive or leader of the organization.

4.3.2 The statement recommended in **4.3.1** and the procurement fraud policy should be communicated to all the organization's personnel and suppliers, and be published on the organization's intranet and public website.

4.3.3 The organization should implement procedures under which:

a) all appropriate and relevant personnel read the procurement fraud policy and agree to comply with it;

b) records are maintained of all personnel who have:

1) received the procurement fraud policy;

2) made the compliance declaration;

c) all appropriate and relevant personnel receive applicable guidance on business ethics, corporate governance or similar.

4.3.4 The organization should prepare a procurement fraud response plan (see **4.12.2**).

4.3.5 The organization should implement procedures by which appropriate disciplinary action (including termination of employment) can be taken against personnel who breach the fraud prevention policy.

4.3.6 The organization should implement an appropriate conflict of interest policy, indicating how it will respond to conflicts of interest, for example:

a) closely monitoring and regulating actual or potential conflicts of interest;

b) observing restrictions imposed by national legislation;

c) not hiring or contracting former public officials in any capacity before a defined period of leaving office;

d) conducting due diligence on staff and suppliers where there is a high risk of conflict of interest, including where individuals can influence selection and award to suppliers (see **A.1**);

e) periodically moving personnel to different positions/roles.

4.3.7 For personnel who could pose a procurement fraud risk to the organization, the organization should implement procedures which:

a) provide that conditions of employment require personnel to comply with the anti-bribery and fraud prevention policies; and

b) give the organization the right to discipline personnel (including termination of employment) in the event of non-compliance.

4.4 Training and awareness

The organization should provide education, training and awareness to all personnel and suppliers who are to be responsible for implementing the procurement fraud controls or who could encounter procurement fraud as part of their duties (and who might not be dedicated procurement staff), to allow them to recognize procurement fraud and make them aware of and understand:

a) the organization's procurement fraud policy, business ethics and code of conduct, and the consequences of any breach of these (see **4.3.5**);

b) the organization's procurement fraud controls;

c) the risk to the organization that can result from procurement fraud;

d) procurement fraud indicators and how such fraud can occur;

e) methods of reporting procurement fraud concerns (including whistleblowing);

f) the organization's procurement fraud response plan (see **4.12.2**);

g) supplier education and awareness of the risks of procurement fraud;

h) the need to ensure there is no interference with the operational independence of staff members exercising a procurement function.

This training should be monitored and repeated at predetermined intervals.

All training that has been provided to and completed by personnel and suppliers should be documented.

The organization should review its fraud prevention policies at defined times or at times outlined within the procurement fraud response plan to confirm that they are up to date and understood by individuals within the organization (see **4.5**).

4.5 Procurement guidance

The organization should prepare and issue guidance on its procurement methods and controls to staff who might be involved in the procurement process (see Annex B).

4.6 Procurement fraud controls

4.6.1 Resources

The organization should provide the resources necessary to implement procurement controls, including personnel, funding and equipment.

4.6.2 Management responsibility

The organization should clearly allocate responsibility for the management of compliance with the procurement controls.

This person (people) should oversee the implementation/management of the procurement system.

4.6.3 Reporting procedures

The organization should implement procedures that:

a) enable personnel to report attempted, suspected or actual procurement fraud, or any breach or weakness within the procurement or procurement fraud controls, to the appropriate person within the organization (either directly or through an appropriate third party);

b) ensure that the organization as far as possible protects the identity of personnel who make confidential reports (unless the organization is required by law to disclose this information in line with the Public Interest Disclosure Act 1998 [2]);

c) allow anonymous reporting (if, and to the extent that, applicable laws allow);

d) protect from retaliation personnel who raise in good faith a concern about actual or suspected procurement fraud or the effectiveness of controls;

e) encourage personnel to seek advice from an appropriate person on what to do if faced with a concern or situation that could involve procurement fraud;

f) provide clear guidance to personnel:

   1) on how to raise a concern about attempted, suspected or actual procurement fraud or the implementation of procurement fraud controls;

   2) assuring them that their reports will be investigated confidentially (in accordance with applicable laws) and acted upon where appropriate, and that feedback will be given where appropriate;

3) on how to access independent advice;

4) on how and when they can report to appropriate external authorities;

g) advise personnel:

1) of their ethical responsibility to report any suspected risk of procurement fraud;

2) of any legal and/or contractual duty to report, and the consequences of any breach of this legal duty;

3) that they will not be at risk of retaliation from the organization for raising in good faith a concern about suspected or actual procurement fraud or implementation of procurement or procurement fraud controls;

4) that their identity will be protected and kept confidential (unless disclosure of identity is required by law);

5) that it is a disciplinary offence to retaliate against someone who in good faith raises a concern about actual or suspected procurement fraud or the implementation of controls.

NOTE 1 These procedures may be the same as, or form part of, those used for the reporting by personnel of other issues of concern (e.g. safety, malpractice, wrongdoing or other serious risk).

NOTE 2 See PAS 1998.

4.7 External reporting procedures

The organization should encourage and facilitate external reporting by existing or potential suppliers or members of the public of attempted, suspected or actual procurement fraud or any breach or weakness within the procurement or procurement fraud controls, to the appropriate person within the organization (either directly or through an appropriate third party) (see **4.4**).

4.8 Security

4.8.1 General

An organization should implement a level of security informed by its risk assessment (see 3.**2**) to protect all data from unauthorized disclosure or access.

4.8.2 Information security

To safeguard against unauthorized disclosure of data the organization should:

a) restrict access within IT systems relating to master vendor data, including tender quotes, unit pricing, competitive bids or any other data, to authorized persons who need to have access for the purposes of fulfilling their role;

b) have guidance in place to ensure data are processed in a secure manner;

c) have an audit capability within IT systems to monitor the distribution of data;

d) have appropriate contractual clauses in place to ensure protection of data throughout the supply chain.

NOTE Requirements of information security management systems are specified in BS ISO/IEC 27001.

4.8.3 Physical security

An organization should implement physical security measures designed to:

a) prevent unauthorized access to equipment, installations, material and data;

b) safeguard against unauthorized removal or dissemination of data;

c) prevent unauthorized access to or tampering with back-up data.

4.8.4 Segregation of duties

The organization should segregate procurement functions throughout the procurement life cycle, including the tendering process, procure-to-pay and contract management. When these functions cannot be separated, a detailed supervisory review of related activities should be put in place as a compensating control measure.

NOTE Segregation of duties is a deterrent to fraud.

Delegated procurement authority controls should be implemented and reviewed on an annual basis.

4.8.5 Asset register

The organization should link all procurement activity to an asset register (see Annex C for the possible contents of such a register).

The register should be audited on a predetermined basis.

4.8.6 Goods received process

The process of receiving, recording and delivering goods from the supplier to the end user should be transparent and auditable.

4.8.7 Vetting

All internal and outsourced staff who are to be involved in the procurement process should be subject to appropriate background checks, e.g. financial checks, confirmation of identity, referee checks and criminal record checks (see **B.2** and BS 7858). Particular attention should be given to:

a) individuals working within the procurement area;

b) those who have influence over the procurement process or access to financial information at a higher-than-usual level;

c) any identified or reported conflict of interest;

d) any breach of the procurement process or related internal policies by staff who work in risk areas;

e) review of the checks at predetermined intervals to ensure that any changes to the information obtained during the background checks are identified, e.g. conflict of interest;

f) promotion or movement to higher risk positions.

4.9 Supply chain security

NOTE The procurement of goods, works or services, at the national and international level, is likely to involve the movement of goods, works or services from a supplier or source to the end customer. An international supply chain has additional levels of complexity.

4.9.1 Supply chains involve various operations, including manufacturing, processing, loading/unloading and transportation (including across international borders). Risk areas that should be considered include:

a) initial point of manufacture, processing or handling;

b) storage locations (warehouses, bonded warehouses);

c) transportation (air, land or sea), including checking the integrity of the goods, e.g. source, packaging, labelling;

d) loading and/or unloading of goods at all points along the supply chain;

e) where goods pass between different organizations;

f) all points where shipping and clearance documentation is generated and handled; and

g) inland transport routes and methods of conveyance.

NOTE Further guidance on supply chain security can be obtained from BS ISO 28000.

4.9.2 The procurement risk(s) associated with each tier of the supply chain should be considered, including how tier 1 suppliers monitor their suppliers.

4.9.3 The organization should implement suitable controls to manage security effectively within the supply chain and thus mitigate potential procurement fraud risk. A person should be designated as responsible for supply chain security, with defined responsibilities and sufficient authority to drive forward recommendations and show, through communication and staff training, that their internal and external controls and procedures provide the necessary security.

NOTE With the threat of terrorism, drug trafficking, human trafficking, counterfeiting and fraud contaminating international trade, many countries and trading blocs are developing countermeasures to ensure that supply chains are and remain secure. The European Union has introduced the Authorised Economic Operator (AEO) as a designation for organizations and companies involved in the supply chain which have proved themselves to be compliant, trustworthy and safe and secure.

4.10 Procurement processes

4.10.1 e-procurement

The use of an e-procurement platform should be implemented where possible to mitigate procurement fraud risk by ensuring that the procurement process is secure, transparent and auditable.

4.10.2 Procurement cards

Procurement cards are generally used for high-volume and low-value purchase of goods, works and services. To support fraud mitigation, the procurement card policy and processes should be transparent and auditable.

4.10.3 Sole source procurement

The organization should define when it would be appropriate to utilize sole source procurement, e.g. a particular vendor has unique expertise that makes it impossible for anyone else to do the work or supply goods, or the services are not available from another source. Sole source procurement should not be used to avoid competitive tendering.

4.10.4 Pre-qualification

The organization should, where practicable, implement a pre-qualification process for suppliers, consultants and subcontractors and, as part of this process, assess the risk of procurement fraud and corruption.

*NOTE This process is also likely to include due diligence. See **4.12** and **B.1**.*

4.10.5 Contractual protections

The organization should ensure that, when drafting and negotiating a contract with a supplier, appropriate legal advice is sought and appropriate contractual protections are included in that contract.

NOTE Examples of such protections are as follows:

a) where a supplier commits an act or omission which results in that supplier committing a procurement fraud:

1) the supplier has an obligation to report that act or omission to the organization;

2) such act or omission is deemed a material breach of contract which allows the organization to exercise a number of remedies (for example, require the supplier to undertake a root cause analysis and implement a remedial plan, require the removal of the supplier personnel or contractor who committed the procurement fraud from the engagement, or unilaterally terminate the contract without any financial penalty);

3) the organization has the right to "step in" until the supplier demonstrates to the organization's reasonable satisfaction that the supplier has remedied the situation;

4) the liability for the supplier flowing from such breach is not capped by the general limitation of liability clause in the contract; and

5) any losses to the organization flowing from such breach are not covered by the exclusion of liability clause (for example, such losses not being categorized as an indirect or consequential loss);

b) the organization having audit rights to ensure that the supplier is in compliance with its legal and contractual obligations to manage and mitigate procurement fraud;

c) the supplier not having an exclusions clause in the contract for avoiding responsibility for procurement fraud.

4.10.6 Framework agreements

To mitigate the procurement fraud risk within framework agreements, the following steps should be taken:

a) a suitable business case and justification should be prepared and then followed before a vendor is approved;

b) due diligence should be conducted on potential vendors to confirm their ability to provide the services specified;

c) it should be confirmed that there are no conflicts of interest within the framework process;

d) category spend should be monitored to identify any irregularities in the amount of spend with each vendor and checked to determine whether vendor spend is outside of the framework agreement with each vendor;

e) a review period for each framework agreement should be agreed to confirm that each vendor is still able to provide the services agreed, i.e. a vendor has not gone into liquidation or traded fraudulently.

4.11 Internal audit

4.11.1 The organization should implement appropriate and proportionate internal audit processes or other procedures that inspect contracts, controls and procedures for any indication of procurement fraud, which might be indicated by:

a) non-compliance with procurement controls;

b) failure by suppliers to comply with the organization's fraud policy requirements;

c) failure by suppliers to comply with their contractual requirements, giving rise to actual or prospective procurement fraud;

d) gaps in controls or implementation of procurement controls.

4.11.2 These audits should be conducted at predetermined intervals by staff who have an understanding of the procurement process. This should be supported as required by no-notice audits conducted as part of the procurement fraud controls where there is a specific area of risk within an organization.

4.11.3 The organization's planned audits should take into consideration the risk and importance of the processes and areas to be audited and the results of previous audits.

4.11.4 Audit reports detailing any significant matters identified, including any recommended corrective actions or improvements, should be provided to the relevant personnel.

4.12 Due diligence

4.12.1 Suppliers

Where the risk assessment shows that a supplier might pose an unacceptable procurement fraud risk, the organization should implement defined and documented procedures to undertake due diligence on the supplier prior to entering into any business relationship with it.

The due diligence should be repeated (as part of a predetermined re-qualification) at a defined frequency during the business relationship so that new information can be properly assessed.

The organization should have in place:

a) a method of assessing each supplier against the organization's procurement standards before placing them on the approved suppliers list;

b) a defined method and timescale of re-qualifying companies on the approved supplier list.

NOTE The frequency of the review depends on the organization's requirements, but is recommended to be at least annually.

4.12.2 Procurement fraud response plan

The organization should identify and publish procedures in which there is a methodical response to allegations or suspicions of procurement fraud with defined responsibilities.

The procurement fraud response plan should be made available to all staff so that they understand their roles and responsibilities when fraud is suspected or identified. The plan should cover such areas as:

a) method of reporting fraud;

b) whistle-blower protection;

c) the organization's investigation response (in outline);

d) response plan owner;

e) internal reporting to departments that have a responsibility within the response structure, including:

   1) internal audit;

   2) compliance;

   3) ethics/legal;

   4) human resources (HR);

   5) internal communications;

f) external reporting to any relevant regulatory body;

g) reporting structures to top management and the risk committee;

h) HR response procedures that can be implemented where a member of staff, consultant or other person they are responsible for is suspected of procurement fraud;

i) accurate record keeping, including decision-making;

j) review of the organization's response to suspected incidents of procurement fraud to determine whether policies and procedures, including the response plan, need to be amended where gaps in the response are identified.

4.12.3 Investigation procedures

The organization should implement procedures which provide for:

a) appropriate investigation by the organization of any procurement fraud allegation or suspicion, or any breach of or weakness identified within the procurement controls; and

b) appropriate action in the event that the investigation reveals procurement fraud or a breach or weakness in the controls.

5 Monitor and review

5.1 Monitoring mechanism

5.1.1 The compliance manager (see **2.1** and **4.7**) should have in place a mechanism through which they can:

a) monitor purchases made by the organization to confirm compliance with the organization's procurement procedures and policies;

b) investigate allegations of procurement fraud;

c) record and report deviations from laid down policies and procedures, and ensure that remedial actions are taken;

d) record sanctions imposed for a breach of procurement policies and procedures.

5.1.2 The compliance manager should assess on an ongoing basis whether the procurement fraud controls are:

a) adequate to manage effectively the procurement fraud risks faced by the organization; and

b) being effectively implemented.

5.1.3 The compliance manager should report at planned intervals to top management on the adequacy and implementation of the procurement fraud controls.

5.1.4 The responsibility, scope and method for planning and conducting audits, and the requirement for reporting results and maintaining records, should be defined in a documented procedure.

5.1.5 Audit reports detailing any significant matters identified, and any recommended corrective actions or improvements, should be provided to the compliance manager and top management.

5.1.6 To ensure the objectivity and impartiality of the audit programme, the organization should, so far as is reasonable, ensure that the audit is undertaken by:

a) an independent function or person within the organization established or appointed for this process; or

b) the compliance manager (unless it is the compliance manager's own actions which are being audited); or

c) an appropriate third party.

5.2 Top management review

5.2.1 In order to ensure the continuing adequacy and effectiveness of the procurement fraud controls, top management should review the scope and implementation of the procurement fraud controls. This review should be carried out:

a) at regular planned intervals; and

b) when major changes to the organization's activities or structures take place.

5.2.2 The review should consider a number of issues, including:

a) breaches/incidents and control weaknesses that have been identified;

b) the compliance manager's assessment and reports (see **5.1.2** and **5.1.3**);

c) audits undertaken (see **4.11**);

d) reports generated by personnel (see **4.6.3**).

5.3 Lessons learned

An organization should implement an information management process to ensure that all material collected from procurement controls and procurement fraud controls that highlights inadequacy or risk within the procurement process is communicated by top management to relevant staff to respond to the risk.

5.4 Improvement of the procurement fraud controls

5.4.1 The organization should implement a procedure for changing or improving the controls whenever this is necessary or desirable following compliance manager or top management review.

5.4.2 All proposed changes and/or improvements should be assessed prior to their introduction, and, if appropriate, actions taken to ensure that they do not reduce the effectiveness of the procurement fraud controls.

Annex A (informative) Types of procurement fraud

A.1 Abuse of contract variations or additional works

Contract variations or submission of additional works requests can be manipulated. Where additional works/variations are requested, this can be susceptible to fraud without the correct monitoring, auditing and authorization processes in place.

A.2 Bid manipulation

An insider can manipulate the bidding process in a number of ways to benefit a favoured contractor or supplier, eliminating the competition. These include accepting late bids, changing bids and re-bidding work. Additionally, selecting poor or inadequate suppliers to submit bids will allow a favoured supplier to win a contract. This corruption could be conducted to support a cartel (see **A.7**), including where the bid evaluation process is being manipulated, i.e. information is left out or the insider is used to rig the bids where new competitors bid that are not part of the cartel.

A.3 Bid rigging

Bid rigging involves organizations colluding to influence a competitive bidding process to secure a predetermined contract award and price.

A.4 Bid rotation

In this scheme, all competitors collude to submit bids, but take turns at being the lowest bidder. Competitors that are part of the cartel can take turns on the winning bid dependent on the size and value of the contract.

A.5 Bid suppression

Here, one or more competitors who would have been expected to bid agree to refrain from bidding or to withdraw a previously submitted bid so that an agreed winning competitor's bid is accepted.

A.6 Bribe

This involves an offer, promise or payment, including the request or receipt of a pecuniary advantage, for the purpose of influencing the procurement process or to allow the illicit overcharging, false invoicing, product substitution or acceptance of substandard goods, materials, works or services within the contract.

A.7 Cartels

A cartel is a collection of organizations that act together to influence prices for certain goods, works and services by controlling production and marketing.

A.8 Complementary (cover) bidding

This bid rigging method is conducted when competitors agree to submit either complementary high bids or to submit a bid with additional terms that they know will not be accepted. These activities give the appearance of competition and are the most common forms of bid rigging schemes. This allows their own pre-selected contractor to win contracts, either on a rotating basis or with the winning contractor sharing the profits between parties.

A.9 False invoicing

This involves the submission of invoices for works, services or goods that were not provided. There are many examples of false invoicing that include duplicate billing, claims made for additional workers who were not present (ghost workers) or abuse of time cards. The costs have not occurred, are not reasonable or cannot be directly or indirectly allocated to the contract.

A.10 Fictitious vendors

Here, fictitious vendors are placed on the supplier's list and false invoices are created and used either to launder corrupt payments to others or to facilitate the theft of monies from the organization.

A.11 Ghost/Shell company

Ghost/Shell companies can be set up or used to bid for tenders and, where contracts are won, monies are asked for up-front before any goods, works or services are provided. The goods, works or services will either not be provided or only partially supplied. Websites can be created to support the appearance of legitimacy of a ghost/shell company. A company can be set up with a name similar to a well-known company and bid for work.

A.12 Inflated claims and mischarging

These practices involve invoicing for higher costs than were actually incurred, including through the increase in quantity of materials used or services provided, or increasing the number of staff or hourly/daily rate.

A.13 Manipulation of delivery

This practice involves delaying the contract delivery to allow additional costs to be incurred.

A.14 Market sharing

Market sharing involves companies dividing markets or product lines and agreeing not to compete against each other. This can occur where products or services are specialist and very few companies globally are involved in the manufacture of the products or provision of the services.

A.15 Price fixing

Once a cartel is in place, it can fix the contracting price by increasing the value of the lowest bid, thereby creating greater profit to share between colluding companies.

A.16 Product substitution

A contractor or vendor substitutes products with material of lesser quality than specified or uses counterfeit, defective or used parts.

A.17 Purchases for personal/resale

An insider purchases items that are intended for their own use, or for resale. In these circumstances the thefts can be carried out for personal use or, as part of organized crime. Goods are identified and stolen to order and a number of individuals might be involved in the acquisition and transportation of the stolen goods. The purchase information is altered, falsified or destroyed to hide the originator of the paperwork.

A.18 Rigged specification

An insider unduly manipulates the specification of an organization's requirement such as to allow a favoured contractor to qualify for a bidding process for which they would not otherwise have qualified or leave that contractor as the only realistic contractor to meet the requirement.

A.19 Split purchasing

Purchases can be split into two or more purchases so that each purchase is below the financial threshold that would require additional financial scrutiny or a competitive tender process.

A.20 Unjustified single/sole source

This involves an insider deliberately writing a non-supportable single source justification to avoid a competitive tender selection and illicitly award a contract to a predetermined vendor.

Annex B (informative) Guidance on procurement methods and controls

*NOTE The guidance in this annex is illustrative only. Its purpose is to indicate in some specific areas the type of actions which an organization may take in implementing its procurement fraud controls. It is not intended to be comprehensive. Nor is an organization required to implement the following steps in order to have compliant procurement fraud controls. The steps which the organization takes need to be reasonable and proportionate, having regard to the nature and extent of procurement fraud risks that the organization faces, and taking into account the factors listed in **4.1**.*

B.1 Due diligence

B.1.1 The purpose of due diligence on a supplier is to establish whether the supplier poses an unacceptable procurement fraud risk to the organization.

B.1.2 Issues that the organization might find useful to identify include:

a) whether, and to what extent, the supplier has procurement fraud controls;

b) whether the supplier (or any of its directors or senior staff):

   1) has a reputation for fraud;

   2) has been investigated, convicted or debarred for procurement fraud;

   3) has a sound financial standing and is able to deliver the contract.

B.1.3 The nature, type and extent of due diligence undertaken depends on factors such as the ability of the organization to obtain information, the cost of obtaining information and the extent of the possible procurement fraud risk posed by the relationship.

B.1.4 A high-risk supplier in a high-risk country is likely to require a significantly higher level of due diligence than a low-risk supplier in a low-risk country.

B.1.5 Particular attention needs to be paid to new suppliers.

B.1.6 The due diligence may include, for example:

a) a web search on the supplier and top management links to the organization;

b) making enquiries of appropriate third parties about the supplier's quality of goods, works or services, including ethical reputation and ability to provide services required;

c) assessing the supplier's involvement or performance in the required service area throughout the procurement cycle.

B.1.7 The supplier can be asked further questions based on the results of the initial due diligence (for example, to explain adverse comments). Appropriate levels of staff need to be involved in this process, from both the supplier and the organization.

B.1.8 Due diligence is not a perfect tool. The absence of negative comment does not necessarily mean that the supplier does not represent a risk. Negative comment does not necessarily mean that the supplier constitutes a risk. However, the results need to be carefully assessed and a rational judgement made by the organization based on the facts available.

B.2 Employment procedures: vetting of personnel

When vetting its personnel, particularly high-risk staff, such as agency staff, the organization may take actions such as:

a) discussing its procurement fraud and anti-bribery policies with prospective personnel at interview, and assessing whether they appear to understand and accept the importance of compliance;

b) taking reasonable steps to verify that qualifications are accurate;

c) taking reasonable steps to obtain satisfactory references from previous employers;

d) conducting checks for criminality (and pending criminal cases), bankruptcy, disqualified directors, etc.;

e) taking reasonable steps to verify that the organization is not employing individuals in return for their having, in previous employment, improperly favoured the organization;

f) ensuring that the purpose of employment is not to secure improper favourable treatment for the organization.

B.3 Gifts, hospitality and expenses

For gifts and hospitality, the procedures implemented by the organization could, for example, be designed to:

a) control the extent and frequency of gifts and hospitality by:

   1) a total prohibition on all gifts and hospitality; or

   2) permitting gifts and hospitality, but limiting them by reference to such factors as:

      i) a maximum expenditure (which may vary according to the territory and type of gift and hospitality);

      ii) frequency (relatively small gifts and hospitality can accumulate to a large amount if repeated);

      iii) timing (e.g. not during tender negotiations);

      iv) reasonableness (taking account of the market and seniority of the giver or receiver);

      v) identity of recipient (e.g. those in a position to award contracts or approve permits, certificates or payments);

      vi) reciprocity (no one in the organization can receive a gift or hospitality greater than a value which they are permitted to give);

      vii) the legal and regulatory environment (some territories and organizations may have prohibitions or controls in place);

b) require approval in advance of gifts and hospitality above a defined value or frequency by an appropriate manager;

c) require gifts and hospitality above a defined value or frequency to be effectively documented and transparent (e.g. in a register or accounts ledger).

NOTE BS 10500 specifies requirements for an anti-bribery management system. Attention is drawn to the corporate liability issues that apply to UK associated business under Section 7 of the Bribery Act 2010 [1] and the potential for acts within an organization's supply chain to confer that liability by association.

B.4 Financial controls

Depending on the size of the organization and the transaction, the financial controls implemented by an organization could include, for example:

a) implementing a separation of duties, so that the same person cannot both initiate and approve a payment;

b) appropriate tiered levels of authority for payment approval (so that larger transactions require more senior management approval);

c) ensuring that the payee's appointment and work or services have been approved by the organization's relevant approval mechanisms;

d) requiring at least two signatures on payment approvals;

e) requiring the appropriate supporting documentation to be annexed to payment approvals;

f) restricting the use of cash;

g) ensuring that payment categorizations and descriptions in the accounts are accurate and clear;

h) implementing periodic management review of significant financial transactions;

i) implementing periodic financial audits;

j) ensuring the procure-to-pay controls are implemented and enforced;

k) ensuring there is no interference with the operational independence of staff members exercising a procurement function;

l) ensuring key staff have a least one significant break from work annually (e.g. two weeks) without participating in work processes.

B.5 Internal audit

B.5.1 The frequency of audit will depend on the organization's requirements. It is likely that some sample projects, contracts, procedures, controls and systems will be selected for audit each year.

B.5.2 The selection of the sample can be risk-based, so that, for example, a high-risk project would be selected for audit in priority over a low-risk project.

B.5.3 The intention of the audit is to provide reasonable assurance to top management that the procurement fraud controls have been implemented and are operating effectively, and to provide a deterrent to any potentially corrupt or fraudulent personnel (as they will be aware that their project or department could be selected for audit).

Annex C (informative)

Asset register

The organization should include such information and data as follows in the form of a register of its assets:

a) identification number or unique reference for the asset;

b) make, model and/or version number;

c) manufacturer;

d) vendor, if different from manufacturer;

e) date of manufacture;

f) date of acquisition, installation or completion of construction;

g) location of asset.

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

BS 10500:2011, *Specification for an anti-bribery management system (ABMS)*

BS EN ISO 9000:2005, *Quality management systems – Fundamentals and vocabulary*

BS ISO 28000, *Specification for security management systems for the supply chain*

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

PAS 1998, *Whistleblowing arrangements – Code of Practice* (freely available as a download from http://shop.bsigroup.com/en/forms/PASs/PAS-1998/Confirmation/ or www.pcaw.co.uk/bsi)

Other publications

[1] GREAT BRITAIN. Bribery Act 2010. London: TSO.

[2] GREAT BRITAIN. Public Interest Disclosure Act 1998. London: TSO.

Further reading

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Bribery in Public Procurement: Methods, actors and counter-measures*. Paris: OECD. 2007.

TRANSPARENCY INTERNATIONAL. *The Integrity Pact: A powerful tool for clean bidding*. Berlin: Transparency International. 2009.

This page deliberately left blank

This page deliberately left blank

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

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

All the data, software and documentation set out in all British Standards and other BSI publications are 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. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. Details and advice can be obtained from the Copyright & Licensing Department.

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.™