BS 8453:2011

BSI Standards Publication

Compliance framework for regulated financial services firms – Specification

bsi.

...making excellence a habit.™

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

ISBN 978 0 580 69207 9

ICS 03.060

The following BSI references relate to the work on this standard:
Committee reference SVS/6
Draft for comment 10/30210204 DC

Publication history
First published February 2011

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 16, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI and came into effect on 28 February 2011. It was prepared by SVS/6, *Financial services*. A list of organizations represented on this committee can be obtained on request to its secretary.

Information about this document

The standard is relevant to all firms providing regulated financial services in the UK. The extent to which the requirements of this standard are applicable to an individual firm depends on the nature, size and complexity of the firm's business.

A compliance framework and the compliance function can cover many different aspects of a firm's control environment. The aim of this standard is not to specify how this is structured, but to indicate that the control environment around compliance risk is established by the governing body after discussions with the compliance function as to how responsibility for identifying and managing the various aspects of compliance risk is apportioned within the firm. The standard is not intended as an instrument for regulation. Rather, it is a tool for compliance functions and professionals. Compliance with the standard is voluntary and firms are at liberty to implement the standard in a way that is relevant, appropriate and proportionate to their business model.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type and are expressed in sentences in which the principal auxiliary verb is "shall". Compliance with the provisions is necessary for compliance with the standard.

Commentary, explanation and general informative material is presented in notes 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.

Compliance with a British Standard does not equate to compliance with legal and regulatory requirements. Users still have to comply with the law.

1 Scope

This British Standard specifies overarching policies, procedures and methods for operating a compliance framework (see Clause **4**) within a regulated financial services firm.

This standard sets out a methodology for implementing and managing the compliance framework at both group and line level.

The extent to which the requirements of this standard are applicable to an individual firm depends on the nature, size and complexity of the firm's business.

NOTE Firms may implement this standard in a way that is relevant, appropriate and proportionate to their business model.

The standard does not specify requirements for risk management, data protection (covered in BIP 0012 and BS 10012), complaints handling (covered in BS ISO 10002), or inclusive service provision (covered in BS 18477).

2 Normative references

The following referenced document is indispensable for the application of this document.

Financial Services Authority (FSA) Glossary (http://fsahandbook.info/FSA/glossary-html/handbook/Glossary)

NOTE It is expected that the definitions in the FSA Glossary will not change when the regulatory framework changes.

3 Terms and definitions

For the purposes of this British Standard, the terms and definitions given in the FSA Glossary and the following apply.

NOTE 1 In particular, the FSA definitions of "approved person", "compliance (oversight) function" (hereafter referred to as "compliance function"), "governing body", "regulated activity" and "senior manager" are adopted by this British Standard. The term "regulated firm" is used in place of the FSA term "regulated entity", but shares the same definition.

NOTE 2 It is necessary to be clear about definitions as this is a potential source of noncompliance.

3.1 compliance
adherence to requirements of the regulatory system that apply to the firm and/or specified individuals within it and the regulated activities which the firm and/or such individuals carry out

3.2 compliance framework
series of activities across a firm that, when implemented together, help to ensure compliance

3.3 compliance monitoring
activity undertaken by a firm to obtain assurance that its systems of control are operating adequately and are managing compliance risks effectively

3.4 compliance risk
potential for legal or regulatory sanctions, material financial loss, or loss to reputation arising from a firm's failure to comply with applicable requirements under the regulatory system that apply to the firm and its regulated activities

3.5 regulator
authority or body responsible for the authorization, regulation and/or supervision of any regulated activities, whether in the UK or overseas

4 Guiding principles

4.1 Compliance culture

The firm's governing body, through policies, example and appropriate training, shall articulate a set of core values which underpin the firm's relationships with its clients (including customers), counterparties, regulatory authorities, industry and markets, and define the behaviours expected of its staff, thereby establishing a compliance culture which promotes integrity in all aspects of the firm's business. A values-led compliance culture shall be evident in the actions, decision-making and communications of the firm, its management and its staff.

*COMMENTARY ON **4.1***
A compliance culture can be promoted by, among other things, mission statements and codes of conduct. The firm's governing body and senior managers should work with the compliance function and others to drive the culture, identify deficiencies in that culture and provide remedies. The respective roles of the governing body and senior managers in the management and oversight of compliance should be clearly and explicitly defined and made known throughout the firm.

4.2 Transparency in dealings with regulators

The firm shall deal with its regulators in an open and cooperative way, including as set out in **5.6**.

4.3 Independence

The compliance function shall be able to demonstrate independence: both independence to act, inspect records, challenge and report, and independence from the business it monitors. In particular, the method of determining remuneration of those involved in the compliance function shall not compromise their objectivity or be likely to do so.

NOTE 1 If a compliance officer supports the whole business of a firm, an element of their remuneration may be based on the profitability of the entire firm, but it should not be the only or dominant metric. Performance may also be based on other, non-financial metrics.

NOTE 2 This standard assumes that a firm has a separate compliance function. Where this is not the case, the term "compliance department" or "compliance function" should refer to the firm's registered CF10.

NOTE 3 A smaller firm should have policies and procedures in place to manage potential conflicts.

NOTE 4 Further guidance is given in:

- *SYSC 6.1.4R(4) [1];*
- *the report of the IOSCO Technical Committee on Compliance function at market intermediaries [2]; and*
- *the Basel report on Compliance and the compliance function in banks [3].*

4.4 Authority

The compliance function shall have sufficient authority from the governing body to allow it to fulfil its responsibilities effectively.

4.5 Adequacy of resources and approach

The compliance function shall have adequate resources, taking into account the nature, scale and complexity of the firm's business. The firm's compliance resources should also be appropriate in terms of, amongst other things, competence and relevant experience of staff, the overall annual budget, IT and training.

NOTE Further guidance is given in :

- *SYSC 6.1 [1];*
- *the report of the IOSCO Technical Committee on Compliance function at market intermediaries [2]; and*
- *the Basel report on Compliance and the compliance function in banks [3].*

4.6 Confidentiality

The compliance function shall maintain the strictest levels of confidentiality when carrying out its duties. Information to which the compliance function has access, such as personal data, disciplinary information, remuneration, legal and regulatory proceedings and new business strategies, shall be treated with appropriate confidentiality.

5 The compliance framework

Objective: To set out the responsibility of the governing body for the management of compliance risk and the establishment, independence and resourcing of the compliance function, according to the nature, scale and complexity of the firm's business.

5.1 Governing body involvement and responsibilities

Managing compliance risk shall ultimately be the responsibility of the firm's governing body, but in a larger firm may be delegated to a sub-committee of the governing body, e.g. a compliance and risk committee. The compliance framework is a key component in managing compliance risks, so the governing body and any senior

managers to whom relevant responsibilities have been delegated by the governing body shall seek to ensure that:

a) compliance risk is managed as an integral, but independent, part of the firm's wider risk management;

b) they understand which business and compliance risks are and are not covered by the compliance framework;

c) the scope of coverage is documented;

d) it is clear who is responsible for business and compliance risks identified in the compliance framework which are not the responsibility of the compliance function (e.g. a firm may have a separate data protection officer);

e) compliance risks are identified and assessed with appropriate frequency;

f) they periodically review, and evidence formal approval of, the compliance framework, having assessed that there are adequate resources to maintain the framework;

g) they define and endorse the objectives and strategy for the compliance function;

h) there is provision for regular reports to the governing body regarding the status of the compliance framework, highlighting progress on open issues or new issues of concern, including areas of work not completed on schedule;

i) appropriate action is taken to address areas of concern or areas of work not completed on schedule and that the actions taken are fully documented;

j) staff cooperate with and assist the compliance function; and

k) they take prompt and appropriate action to address and resolve issues escalated to them by the compliance function.

*COMMENTARY ON **5.1***
While significant responsibilities will be apportioned among the firm's senior managers, the governing body is ultimately accountable as it is responsible for overseeing senior managers' management of compliance.

5.2 Compliance risk assessment and management

Objective: To establish the accountability for compliance risk and the principles behind its identification, measurement, management and reporting.

The governing body shall be accountable for and manage compliance risk.

*COMMENTARY ON **5.2***
Compliance risk assessment is an important element of any compliance framework and is regarded along with other risks, such as market risk, insurance risk, credit risk, liquidity risk, group risk, insurance risk and other aspects of operational risk, as an important risk to identify, measure and manage. The firm's arrangements should reflect the nature, scale and complexity of its business. This requires the firm to understand its specific regulatory context and to make some assessment of its compliance risk profile given its products, client base and operational geography.

In identifying and addressing its compliance risk, the firm may take the following steps.

a) Determine and apply risk factors

Risk factors, which might include the following, are routinely identified.

- *The types of client with which the firm deals.*
- *The nature of the markets and industry in which the firm operates.*
- *The nature of the services the firm offers and/or the products in which the firm deals.*
- *Current regulatory requirements and concerns.*
- *Relevance of the business or products to the regulators' statutory objectives.*
- *The extent to which the business or sector in question has had compliance issues in the past.*

On each determination, the risk factors are applied to the different business areas to assess the level of compliance risk currently faced by these areas. A robust risk rating methodology, which is not necessarily complex, is applied regularly on a consistent basis.

b) Manage compliance risk

On each routine assessment of the current risk factors and application of the risk rating methodology to the firm's businesses, the firm has a current measure of the compliance risk associated with each activity. This should be used to inform:

- *the level of compliance advisory resource to be allocated to that business line;*
- *the amount and level of compliance monitoring to be applied to transactions and products in that business line;*
- *the amount and type of training to be provided to that business line.*

c) Report compliance risk to the governing body

The compliance function routinely reports the assessment of the firm's compliance risk, and any change to this assessment, to the governing body at regular intervals. The compliance function is usually responsible for both the compliance risk assessment and for reporting compliance risk at regular intervals. Reporting may include:

- *an assessment of the level of compliance risk in all business areas, highlighting any changes from the firm's initial assessment (see **5.1**);*
- *a report of risks identified during interactions with the regulators;*
- *an update on all regulatory initiatives, such as policy developments and key areas of regulatory scrutiny; and*
- *a report on all internal matters which materially impact on the management of compliance risk, or have the potential to do so.*

5.3 Advice

Objective: To establish policies and procedures for the delivery of compliance advice.

The compliance function shall develop policies and procedures for the provision of compliance-related advice on, amongst other things:

a) dealing with specific requests for advice and issuing proactive advisory compliance communications; and

b) establishing how compliance advice can be obtained.

*COMMENTARY ON **5.3***
The firm may distinguish, and provide separate detail on, business areas in which compliance advice is frequently needed, including advice on:

- *regulatory requirements and internal compliance policies;*
- *implementing legal and regulatory requirements through the firm's policies and procedures;*
- *the regulatory implications of new products and business developments;*
- *business-specific compliance advice; and*
- *training and education.*

The firm may also identify the key considerations in respect of different types of compliance advice and different types of audience (e.g. methods of delivery, style) in areas such as:

- *the issuing of proactive advisory compliance communications (e.g. oral briefings at morning meetings, email alerts and "lessons learnt" briefings);*
- *advising senior managers and the governing body;*
- *providing and coordinating advice in relation to regulatory incidents and their remediation;*
- *regulatory, supervisory and enforcement requests; and*
- *obtaining, where appropriate, external advice (e.g. from lawyers or consultants) and related factors to consider (e.g. the extent of legal privilege, regulatory expectations).*

The firm should also consider the option of documenting "material" advice given or received to provide a contemporaneous record.

5.4 Compliance monitoring

Objective: To set out the standards to be applied to the compliance monitoring work undertaken within a firm following the decisions on planning and allocation.

The compliance monitoring programme shall be derived from the decisions on planning and allocation based on the compliance risk assessment. Judgements regarding how compliance risks are to be monitored and the frequency of monitoring shall be based on the compliance risk assessment.

In order to demonstrate that it is monitoring its compliance risks, the firm shall record key information in the form of written or electronic working papers or systems-generated exception reports. These records shall be retained in an accessible format in compliance with an approved retention schedule and in an authentic, reliable and trustworthy form.

*COMMENTARY ON **5.4***
The information recorded can include any of the following.

a) Details of the monitoring work to be undertaken and the risk(s) being monitored.

b) The frequency of the monitoring work.

c) The date the monitoring work is undertaken.

d) The person responsible for undertaking the monitoring work and any person responsible for reviewing the monitoring work.

e) A detailed record of the monitoring undertaken and particularly the documentation and other evidence examined.

f) An assessment of the results of the monitoring work: in particular, whether any non-compliance is indicative of an absence of or breakdown in the firm's systems and controls or is an isolated error.

g) Documented actions arising in respect of results of the assessment, with evidence that the actions have been taken.

h) Periodic reports for submission to the governing body, detailing:

1) the progress of implementing the monitoring programme against the agreed programme; and

2) all significant compliance failings identified by the compliance monitoring programme, together with the actions taken/to be taken to address these and the person responsible for this.

In determining the adequacy of resources and the necessary level of compliance monitoring, the governing body needs to have regard to the fact that part of the work undertaken by a compliance function cannot always be planned in advance as it is "event driven". Invariably there will need to be a "contingency" within the resource allocation and monitoring programme to meet unexpected and/or future events or to address issues arising from the results of the compliance monitoring.

5.5 Compliance training

Objective: To set out the basis for identifying, developing and delivering essential compliance training within the firm.

*COMMENTARY ON **5.5***
The creation and delivery of a compliance training plan is one element of the firm's overall training and competence programme designed to satisfy the firm's regulatory obligations for training and competence.

5.5.1 Scope of compliance training plan: subject matter

As part of its overall training and competence programme, the firm shall develop a compliance training plan that underpins its compliance culture. In doing so, the firm shall identify appropriate training requirements for staff, by role, line or other categorization and by experience and length of service, and communicate these together with applicable internal policies and procedures.

NOTE An example of an area where training is mandatory is the requirement to provide regular anti-money laundering training for "relevant employees" under the Money Laundering Regulations 2007 [4]. Examples of areas where training is deemed appropriate include the introduction of new regulatory requirements or identified internal deficiencies.

5.5.2 Scope of compliance training plan: employees

The firm shall seek to ensure that all appropriate staff, including senior managers and the governing body, are covered by the training plan.

NOTE Depending on the organization, "staff" can include full-time employees, contractors, temporary staff, appointed representatives, and outsourced/third party service providers. The firm should endeavour to ensure that contracts with its third party providers require them to provide appropriate compliance training where such training is necessary to assist in managing the firm's compliance risk.

5.5.3 Compliance training delivery methodology

The firm shall select the most appropriate training delivery methodology for the nature of the compliance training to be provided and the category of staff to whom it will be provided (taking into consideration the level of knowledge the staff already hold).

NOTE Consideration may be given to a variety of delivery mechanisms, including computer-based training, external courses, in-house classroom delivery, on-the-job coaching and the distribution of bulletins and other reading material.

5.5.4 Responsibility and accountability

The firm shall assign responsibility for the compliance training plan under the compliance programme to an appropriate person. Such responsibility shall include:

a) the development and implementation of the compliance training plan, as well as an assessment of its effectiveness and the introduction of modifications as appropriate; and

b) ensuring that the compliance training plan is approved by the governing body or an appropriate senior manager.

5.5.5 Nature of compliance training for different categories of staff

The firm shall assign to each staff member covered by the training plan compliance training appropriate to the level of understanding/knowledge needed for their role. In assigning the compliance training, the firm shall also specify the time frame within which the compliance training is to be completed and any score that has to be attained to complete the training if it comprises a tested element. The firm shall seek to ensure that the training meets the needs of staff who are covered by any regulatory training and competence requirements or other continuing professional development programmes.

5.5.6 Periodic review

The firm shall keep its compliance training plan under periodic review in terms of content, staff coverage, delivery methodology, time frames and, where appropriate, target scores. Any necessary enhancements and adaptations to the compliance training plan shall be implemented on a timely basis. Additionally, a record shall be maintained of all relevant training undertaken by the firm's employees.

5.6 Regulatory relations

Objective: To promote the development and maintenance of a cooperative and transparent relationship with the firm's regulators.

*COMMENTARY ON **5.6***
Although the governing body is ultimately accountable, in practice, the task of maintaining day-to-day regulatory relations is usually delegated to an appropriate member of the compliance function who, depending on the

nature, scale and complexity of the firm, may either coordinate contact with regulators or act as a single point within the firm. This sub-clause assumes that this task has been delegated. Where this is not the case, it is important that communications with the regulators be properly coordinated by the most appropriate member of the firm's senior management.

5.6.1 Governing body and senior manager commitment

The governing body and senior managers shall demonstrate a commitment to upholding a cooperative and transparent relationship with the firm's regulators (see **4.2**), such that a proactive approach to sharing information can be evidenced.

This can include:

a) maintaining a regular dialogue with day-to-day supervisors and/or other regulatory staff with whom it communicates; and

b) ensuring timely and accurate responses to requests for information.

NOTE This is applicable proportionately according to whether the firm is directly "relationship managed" or has no dedicated day-to-day supervisor, but which might have contact with supervisors through thematic visits. It is good practice to keep records of "material" communications with regulators.

5.6.2 Briefing the governing body and senior managers on regulatory expectations [see also 5.8.2c)]

The firm shall put in place a process, under which the compliance function regularly briefs the governing body and senior managers on the expectations of the regulators. The compliance function shall monitor and obtain information concerning these expectations, e.g. through its own interaction with the regulators, through communications from and materials published by the regulators, and through meetings with professional advisers, trade associations, etc.

5.6.3 Keeping regulators informed of developments/sharing information

As part of its ongoing relationship with the regulators, the firm shall seek to ensure that the regulators are provided with information that they request and are informed of any material developments within the firm of which the regulators would reasonably expect notice.

*COMMENTARY ON **5.6.3***
Material developments (which the firm may also wish to discuss with the regulators or be required to report) can include:

a) significant changes in management or structure;

b) plans to enter new jurisdictions, markets or product areas or to cease lines of business; and

*c) issues (see **5.6.5**) or matters which have a serious regulatory impact [for example, as set out in the FSA's Supervision Handbook (http://fsahandbook.info/FSA/html/handbook/SUP)].*

5.6.4 Managing regulatory inspections/visits

The firm shall ensure that an appropriate member of the compliance function or relevant business area, overseen by the governing body (see

commentary on **5.6**), is tasked with managing preparations for routine or ad hoc regulatory inspections/visits and addressing any issues raised.

NOTE This could include, for example, ensuring that:

a) key personnel are accessible or available for interview;

b) affected parts of the firm have been advised of any inspection/visit by the regulators and the programme agreed in advance;

c) documentation is available for review;

d) appropriate access to systems is provided;

e) information requested in advance by the regulators is provided in a timely and user-friendly format;

f) issues identified or remedial action required by the regulators are discussed, reviewed and agreed;

g) any necessary remedial action taken is sufficient to address issues identified by the regulators;

h) agreed timescales for correcting issues are met;

i) ongoing controls are put in place, or controls improved, to prevent the issue recurring; and

j) a full documentary record of all actions taken is maintained, and submitted to appropriate senior managers and, if requested, the regulators.

5.6.5 Escalating issues to the regulators (see also 5.8)

The firm shall put in place a process to escalate to the regulators issues that materially affect or have the potential to materially affect the firm's compliance with regulatory requirements.

*COMMENTARY ON **5.6.5***
Such issues can include:

a) actual issues or breaches that have been identified and details of the process by which such breaches, risks or issues have been assessed and reported within the firm;

b) material risks that could result in a breach;

c) remedial action to address the actual or potential issue;

d) issues which have arisen in the public domain and could adversely affect the reputation of the firm.

Approaches to the regulators should be timely, but the firm may consider what remedial action would be appropriate prior to alerting the regulators.

5.7 Policies and procedures

Objective: To promote the implementation of appropriate policies and procedures to familiarize staff with the regulatory standards with which they have to comply.

5.7.1 Applicability of policies and procedures

The firm shall ensure that its policies and/or procedures are designed to enable it to meet regulatory requirements. Specifically, the firm shall identify areas in which a formal policy or procedure is mandatory,

although the implementation of policies and procedures need not be limited to such areas.

NOTE Examples of areas in which policies are mandatory include, but are not limited to, complaints-handling (see BS ISO 10002) and conflicts of interest.

*Not all regulatory policies and procedures are maintained by the compliance function. This should be borne in mind when reading **5.7.2** to **5.7.4**.*

5.7.2 Preparation, maintenance and periodic review of policies and procedures

The firm shall allocate to an appropriate person, such as a staff member with relevant experience or a third party service provider, responsibility for preparing and maintaining each regulatory policy and procedure, taking account of the input and comments from relevant parties within the firm.

The policies and procedures shall be made readily accessible, e.g. via the firm's intranet.

The firm shall maintain its regulatory policies and procedures under periodic review so that they continue to remain compliant with regulatory requirements and consistent with the firm's business model and practice. As appropriate, regulatory policies and procedures shall be introduced, amended or withdrawn.

NOTE It might also be appropriate to benchmark draft documents with relevant (e.g. trade association or external advisor) guidance.

5.7.3 Governance of policies and procedures

The firm shall implement a governance structure for the management of its regulatory policies and procedures. This structure shall govern how each document is to be approved, how amendments are to be authorized, the person/body responsible for each policy and procedure and the required review frequency for each document. The firm shall also implement appropriate arrangements for assessing and taking appropriate actions for material breaches of its regulatory policies and procedures.

5.7.4 Regulatory changes

The compliance function shall have in place a policy or process for:

a) keeping up-to-date with actual or potential changes in regulation,

b) communicating these to the relevant areas, such as business lines, risk management, senior managers and the governing body, and to operational management, which is responsible for implementing regulatory changes.

The compliance function shall ensure that appropriate changes to policies and procedures take place in a timely fashion.

NOTE Where there are multiple business lines, the firm might need to consider whether it would be appropriate to establish a network of dedicated compliance staff to stay up-to-date and communicate changes that are relevant to their specific business area.

5.8 Compliance reporting

Objective: To establish and maintain a reporting framework for providing assurance and keeping senior managers and the governing body aware of compliance issues.

5.8.1 Recipients of reports

The firm shall identify the recipients of necessary compliance reports and information.

NOTE Depending on the nature, scale and complexity of the firm, these may include risk committees, compliance committees, audit committees, boards and other compliance or governance decision-making forums.

5.8.2 Reporting process

The firm shall develop a reporting process to keep senior managers and the governing body aware of compliance issues, providing assurance that compliance issues are being addressed, that compliance controls are operating as intended, and that the compliance culture and framework are effective. This shall be aligned with any wider, overall reporting process that is in place within the firm. The governing body shall directly, or through an appropriate member of the compliance function to whom responsibility is delegated, determine and provide the resources necessary to operate and maintain the reporting process, and demonstrate ownership and accountability for the process and content. The firm shall ensure that authors of reports are available to discuss and expand on the content of reports where required by recipients. Key considerations for the reporting process shall include the following.

a) Quality of reporting

The firm shall ensure that its internal and external reports are of an appropriate quality and contain adequate information to enable their audiences to understand the content and to make decisions or request/direct further action. The reports shall have the following qualities.

1) Timely.

   EXAMPLE: Up-to-date and provided sufficiently in advance of key meetings to enable recipients to prepare and make decisions.

2) Of appropriate frequency.

   EXAMPLE: Provided at sufficiently regular intervals with a clear timetable for publication.

3) Targeted.

   EXAMPLE: Concise, containing an appropriate level of detail for the audience.

4) Reliable.

   EXAMPLE: Contain accurate and reproducible information and, possibly, sources of underlying data.

5) Clear.

   EXAMPLE: Easily understood without the need for additional explanation or reference and providing a clear audit trail, including report date, author and recipients.

6) Well structured.

EXAMPLE: Clear format, including calls to action requiring management awareness or action.

7) Objective.

EXAMPLE: Not contain inflammatory or emotive language.

b) Internal awareness of compliance issues

Reports produced for internal audiences shall contain information on potential or actual issues that could materially affect the firm's compliance with regulatory requirements. The reports shall provide detail of such issues, the effects or risks that they pose, action that is being taken to address and/or investigate the issues, and, where determined, details of ownership for addressing the issues and timescales for their remedy.

NOTE The reports may also include:

1) information to provide assurance that the firm is complying with regulations in light of regulatory developments or changes, or changes in the firm's operating environment or market;

2) evidence or confirmation that adequate controls are in place or key compliance controls are operating as intended; and

3) information to demonstrate that compliance risks are, where appropriate, being mitigated and appropriately managed.

c) Internal awareness of regulatory developments (see 5.6.2)

A process shall be put in place to make senior managers, the governing body and relevant internal audiences aware of both national and, where relevant, international regulatory developments. This can include:

1) potential and actual changes to relevant regulations;

2) relevant documents published by regulators or relevant industry bodies that the firm needs to be aware of or respond to;

3) changes to the supervisory process; and

4) compliance weaknesses that have come to light within the firm's peers or sector.

d) Escalating issues to the compliance function and the governing body

The firm shall put in place a policy and procedure to escalate any compliance issues that arise within the firm, such as risks or control breakdowns, to the compliance function or appropriate senior management. The policy and procedure shall provide for the compliance function to escalate material issues to the governing body and enable staff to bypass internal parties and report directly to an independent party, such as an audit committee, where necessary.

e) Monitoring and reporting progress of remedial action

The firm shall put in place a process to track and report any remedial action implemented to address compliance issues or weaknesses. The results of monitoring or implementing remedial action shall form part of reports to senior managers. Delays or deviations from intended actions shall be clearly highlighted.

NOTE Separate reporting processes could be required for whistleblowers under the Public Interest Disclosure Act 1998 [5].

5.8.3 Mandatory reporting to the regulators (see 5.6)

The governing body shall ensure clarity of responsibility for all mandatory reporting requirements, including routine and ad hoc reports and those necessary to meet regulatory requirements.

5.9 Compliance function: controls and supervision

Objective: To set out the basis for the compliance function to establish its own escalation and operating procedures.

The compliance function shall, as appropriate to the nature, scale and complexity of its business, develop, implement and/or monitor relevant policies for the compliance function for identifying, investigating and escalating exceptions/possible regulatory breaches.

The compliance function shall have operating procedures and relevant internal controls for supervising the performance of any compliance tasks that have been delegated for example to the business and document and evidence such supervision.

*COMMENTARY ON **5.9***
In developing escalation procedures for its compliance function, a firm might need to consider, among other issues:

a) independence, conflicts of interests and procedures for their management;

b) data security (particularly with respect to market sensitive information);

c) work processes (including feedback to the business and resolution and follow-up of issues);

d) departmental staff supervision, training and assessment;

e) accountabilities and reporting lines; and

f) contingency planning, e.g. insolvency of major counterparty, notifications to insurers, internal fraud, urgent requests from regulators or law enforcement agencies.

A firm may also assess the effectiveness of its compliance function using internal audit or a third party. See the report of the IOSCO Technical Committee on Compliance function at market intermediaries, "Assessment of the Effectiveness of the Compliance function" [2] and the Basel report on Compliance and the compliance function in banks [3].

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 10012, *Data protection – Specification for a personal information management system*

BS 18477, *Inclusive service provision – Requirements for identifying and responding to consumer vulnerability*

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

BIP 0012, *Data Protection – Guide to practical implementation*

Other publications

[1] FSA. SYSC 6.1, *Senior Management Arrangements, Systems and Controls: Compliance*

[2] IOSCO. Report of the IOSCO Technical Committee on Compliance function at market intermediaries. March 2006. (Available at: http://www.amvcolombia.org.co/attachments/data/20100630220429.pdf)

[3] BASEL COMMITTEE ON BANKING SUPERVISION. The Basel report on Compliance and the compliance function in banks. April 2005. (Available at: http://www.bis.org/publ/bcbs113.pdf)

[4] GREAT BRITAIN. The Money Laundering Regulations 2007. No. 2157. London: The Stationery Office.

[5] GREAT BRITAIN. The Public Interest Disclosure Act 1998. London: The Stationery Office.

Further reading

BS ISO 22222:2006, *Personal financial planning – Requirements for financial planners*

FSA Supervision Handbook. (Available at: http://www.fsa.gov.uk/pubs/hb-releases/rel67/rel67sup.pdf)

FINANCIAL SERVICES SKILLS COUNCIL/INTERNATIONAL COMPLIANCE ASSOCIATION. National Occupational Standards for Compliance and Anti-Money Laundering. 2006. (Available at: http://www.int-comp.org/attachments/aml-standards.pdf)

This page deliberately left blank

This page deliberately left blank

British Standards Institution (BSI)

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

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

About us

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

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

Information on standards

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

Buying standards

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

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

Subscriptions

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

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

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

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

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

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

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

Revisions

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

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

Copyright

Useful Contacts:

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

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

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

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

bsi.

...making excellence a habit.™