

BS 8453:2011



BSI Standards Publication

Compliance framework for regulated financial services firms – Specification

bsi.

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

Publishing and copyright information

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

© BSI 2011

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

Foreword *ii*

1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Guiding principles	2
4.1	Compliance culture	2
4.2	Transparency in dealings with regulators	2
4.3	Independence	2
4.4	Authority	3
4.5	Adequacy of resources and approach	3
4.6	Confidentiality	3
5	The compliance framework	3
5.1	Governing body involvement and responsibilities	3
5.2	Compliance risk assessment and management	4
5.3	Advice	5
5.4	Compliance monitoring	6
5.5	Compliance training	7
5.6	Regulatory relations	8
5.7	Policies and procedures	10
5.8	Compliance reporting	12
5.9	Compliance function: controls and supervision	14
	Bibliography	15

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