

Financial Services Authority

# Operational risk systems and controls

Feedback on CP142

March 2003





# Contents

1	Executive summary	3
2	Introduction	5
3	Feedback on responses to Consultation Paper 142 (CP142)	7
4	Next steps	16

**Annex 1:** List of non-confidential respondents to CP142

This policy statement reports on the main issues arising from Consultation Paper 142 Operational Risk Systems and Controls.

Enquiries can be addressed to:

Lisa Wild  
Prudential Standards Division  
The Financial Services Authority  
25 The North Colonnade  
Canary Wharf  
London E14 5HS  
Telephone: 020 7676 5854  
Fax: 020 7676 5855  
E-mail: CP142@fsa.gov.uk

**It is the FSA's policy to make all responses to formal consultation available for public inspection unless the respondent requests otherwise.**

# 1 Executive summary

- 1.1 In July 2002, we published for comment *Consultation Paper 142* (CP142). It outlined some new draft guidance on operational risk systems and controls for both **SYSC** (one of our high level sourcebooks, entitled *Senior Management Arrangements Systems and Controls*) and **PRU** (our forthcoming *Integrated Prudential Sourcebook*).
- 1.2 The draft guidance for **SYSC** was designed to highlight some of the main areas that a firm should consider when managing operational risk. In so doing it covered a range of topics, including people risk; IT systems and information security; business continuity management; and outsourcing.
- 1.3 The draft guidance for **PRU** was designed to provide some additional guidance to firms on the policies and procedures that they might put in place to identify, assess, monitor and control their operational risks in a prudential context.
- 1.4 Interest in this Consultation Paper has been high. We received 50 responses, from a mixture of authorised firms (both large and small), consultants and trade associations, and other interest groups. The majority of these respondents confirmed that the stated policy was appropriate in terms of the areas covered and the level of detail. In addition, few of these respondents suggested that we should make any material revisions to our proposed policy.
- 1.5 Therefore, the main purpose of this Policy Statement is to indicate that we do not propose to make any significant amendments to the draft text that we outlined in CP142. Our assertions in CP142 – that we felt that the proposed policy was compatible with our statutory objectives, and is the most appropriate way of meeting those objectives – remain unchanged. Also, we feel that the arguments set out in the CBA for CP142 remain valid.

- 1.6 We will issue the final draft of our operational risk systems and controls policy for **PRU** and **SYSC** (the 'near-final' text) later this year. We will issue this along with all our other new policy on systems and controls for market, credit, liquidity, group and insurance risk.
- 1.7 We are grateful to respondents for their useful and informed comments. In this paper we provide a summary of responses received, and our feedback on these responses. We also give a brief update on the international initiatives that are relevant to this area, and an indication of the timeline for future developments.

### **Consumers**

This Policy Statement will be of some interest to retail consumers, because our guidance on operational risk systems and controls is designed to promote our consumer protection objective.

# 2 Introduction

## Background

- 2.1 We received industry feedback to our initial proposals for rules and guidance on operational risk in Consultation Paper 97 *Integrated Prudential Sourcebook* (CP97). We took into account this feedback, as well as changes in our own thinking, and redrafted this text. We then consulted on the revised version in Consultation Paper 142 *Operational risk systems and controls* (CP142) in July 2002. In CP142, we outlined our new proposals for guidance on operational risk systems and controls and outsourcing, and, as part of this revision, we proposed to include some guidance on operational risk in two parts of our Handbook.
- 2.2 First, and as originally intended in CP97, we included some guidance in **PRU**, our forthcoming *Integrated Prudential Sourcebook*. This guidance covers the policies and procedures that a firm should consider putting in place to help identify, assess, monitor and control operational risk in a prudential context. As such, this guidance is specifically concerned with maintaining the solvency of firms and only applies to those firms that represent a threat to our objectives in this context. (These firms include deposit takers, insurers and investment firms that take principal positions or hold client money.)
- 2.3 Second, we included a new chapter on operational risk in **SYSC** (*Senior Management Arrangements, Systems and Controls*). This guidance outlines the main areas that a firm should consider when managing its operational risks and provides some specific guidance on topics such as information security, business continuity management and outsourcing. In contrast to the policy in **PRU**, this guidance will apply to almost all regulated firms (since all firms will face operational risk in some form or another). It is designed to emphasise that operational risk may cause direct losses to consumers as well as to firms.
- 2.4 Interested parties may also wish to review Guidance Note P3 (*Systems and Controls in Insurers*) in the *Interim Prudential Sourcebook for Insurers*. This

note came out of Consultation Paper 140 *The Interim Prudential Sourcebooks for Insurers and Friendly Societies and the Lloyd's Sourcebook: Guidance on Systems and Controls*. Guidance Note P3 includes some material on a number of operational risk related topics such as outsourcing and legal risk.

## **Purpose of this Policy Statement**

- 2.4 This Policy Statement summarises the responses that we received on our proposed guidance in CP142, and advises you of any subsequent changes that we intend to make in the light of these responses.

## **Structure of this Policy Statement**

- 2.5 Chapter 3 contains a summary of the feedback that we received, and our response in each case. Chapter 4 explains what the next steps in the process will be, and provides an update on related international developments. Annex 1 provides a list of non-confidential respondents.
- 2.6 We are grateful to all respondents for their comments. While it is not possible to address in detail every single comment, we will make every effort to take these into account in both our final text and our future work in this area.

# 3 Feedback on CP142

- 3.1 This chapter provides a summary of the responses that we received to CP142 together with our replies to those responses.

## General feedback

- 3.2 Operational factors, such as poor staff training levels, inadequately managed processes and systems, significant changes affecting the business and the outsourcing of certain functions, can have many consequences. The Financial Services Consumer Panel suggested that we should make it clearer in the guidance that one of the main ones is that a firm may not be able to give customers the standards of service and protection that they might reasonably expect.

**Our response:** We take note of the comments made by the Financial Services Consumer Panel, and will make further references to consumers in the final guidance.

One of the key factors behind our decision to include some guidance on operational risk in SYSC was our desire to stress the importance of consumers in this area. In particular, we wished to highlight that operational events may have an adverse effect not only on the value of a consumer's deposits and assets but also on the ability of a firm to discharge its obligations to consumers.

## Specific feedback

Q1: Do you agree that we should use guidance rather than rules when setting out our systems and control policy for operational risk? Does the guidance in Annexes B and C of this CP contain the right amount of detail?

- 3.3 There was a high level of agreement for this approach, and a clear majority of respondents felt that we gave the right level of detail. However, some

respondents, including the FSA Small Business Practitioner Panel, were concerned that supervisory staff would apply the guidance as if it were rules in any case, thereby negating the flexibility of using guidance instead of rules.

**Our response:** We are pleased that our decision to use guidance has met with such approval and will maintain this approach when finalising our Handbook text on operational risk systems and controls. Regarding the application of this guidance to firms, we remain committed to providing a fair and consistent application of our Handbook and policies to regulated firms. We intend to introduce thorough training for appropriate members of our supervisory staff on all eventual Handbook changes. This includes emphasising the significance of the different treatment to be applied to those sections of the revised Handbook that constitute guidance rather than rules.

Q2: Do you agree that it is right to include guidance on operational risk management systems and controls in SYSC?

- 3.4 Most respondents agreed that guidance should be included in **SYSC**, and that this guidance should apply to a wider range of regulated firms than that contained in **PRU**. Certain respondents, however, felt that dividing this guidance between different sections of the Handbook may be confusing to some, and that either collating all relevant guidance in one area, or providing more explicit cross-referencing would be advantageous.

One respondent representing an industry body felt that the existing guidance in **SYSC** was sufficient, and that it was not appropriate to introduce any further guidance at this time.

Another respondent representing an industry body felt that a section of the draft text was suggesting that a firm would need to construct an operational risk profile of the risks faced by both “a firm and its clients” (see PRU 6.1.11G (1) in CP142). This was felt to be unacceptable, as it would be very difficult to profile the operational risks that are faced by a firm’s clients.

**Our response:** We intend to stick with our proposal in CP142 to locate part of our guidance on operational risk systems and controls in SYSC and part in PRU. Each of these pieces of guidance has a different purpose and we do not feel that it would be appropriate to combine them. However, we will look at whether it may be possible to improve navigation between these two pieces of guidance with even better cross referencing and clearer purpose sections.

We do not agree that the existing guidance in SYSC is enough. As with most of the respondents to CP142 we feel that operational risk is a sufficiently important area to warrant some additional guidance.

We do not intend to imply that a firm should construct an operational risk profile of the risks posed to its clients. We intend only to prompt firms to consider the impact of potential operational risk systems and control failures within the firm upon its clients. We will clarify this point in the final ‘made’ text.

Q3: Do we cover the right issues in our operational risk policy on the management of a firm's employees? Is this guidance appropriate in terms of its quantity and depth of detail?

- 3.5 The majority of respondents who answered this question agreed that the right issues were covered, and that the level of detail provided was appropriate. Certain respondents queried the feasibility of being able to exert control over the staff of a third-party supplier, especially in the case of a smaller firm who may not wield the same bargaining power as a larger entity.

**Our response:** We appreciate that it may not be possible, or indeed desirable, for a regulated firm to exercise direct control over the staff of a third-party supplier in all situations. But we would expect a regulated firm to make every effort to satisfy itself that such staff are subject to broadly comparable standards of operational risk controls and considerations. We will revise our guidance to clarify this position more fully.

Q4: Do we cover the right issues in our operational risk policy on the management of systems and processes? Is this guidance appropriate in terms of its quantity and depth of detail?

- 3.6 The majority of respondents who provided feedback on this question felt that the right issues were covered and that the level of detail was appropriate. Some respondents requested more detail on the specific business processes that should be considered when following this guidance. It was also suggested that our guidance on documentation (**SYSC 3A.5.6 to 3A.5.8**) should be moved to before our guidance on IT systems (**SYSC 3A.5.3 to 3A.5.5**). This would be to avoid the implicit assumption that it referred only to IT documentation.

**Our response:** Given the diverse character of operational risk, we do not wish to be overly prescriptive on the business functions that should be considered in relation to the management of a firm's systems and processes. Also, we do not wish to specify the priority that particular business processes should be given and the specific level of effort that should be expended on particular issues. Our use of guidance places the responsibility on management to decide what is and what is not appropriate.

With regard to the suggested amendment to the layout of **SYSC 3A.5**, we intend to incorporate this change into the final text.

Q5: Do we cover the right issues in our policy on business continuity management? Is this guidance appropriate in terms of its quantity and depth of detail?

- 3.7 There was a high level of agreement that the right issues were covered, and to the correct level of detail. Some respondents sought additional guidance on what we considered to represent best practice in terms of the regularity and extent of testing, ideal recovery time targets, and minimum service levels from external vendors.

**Our response:** We are pleased that our policy on business continuity has met with such approval. We feel that the further guidance suggested by some respondents would prove too prescriptive for most firms and so we will keep the existing level of detail.

We are conscious that some firms believe that we will interpret our proposed guidance on business continuity in a prescriptive way. We would like to reassure these firms that we have no intention of being prescriptive and, as with all our guidance, we will apply it in a proportionate way. Our policy on business continuity is designed to be flexible and to be interpreted in accordance with the nature, scale and complexity of a firm's activities.

Q6: Are we right to rely on guidance in our policy on outsourcing?

- 3.8 Most respondents agreed that the use of guidance is appropriate here: it will allow firms to adopt a flexible approach to the management of their outsourcing arrangements that is in accordance with their own particular situation.

**Our response:** We are pleased that this approach has met with such approval, and will maintain this approach in the final text.

Q7 Do we cover the right issues in our policy on outsourcing?  
Is this guidance appropriate in terms of its quantity and depth of detail?

- 3.9 Of the respondents who answered this question, the majority felt that the right issues were covered and that the level of detail was appropriate. It did, however, elicit several requests for further guidance. For example, some respondents requested further guidance on the activities that are included in our definition of outsourcing (e.g. on whether joint ventures and franchising are included). A few respondents also asked for more guidance on how to determine what should be considered 'material' outsourcing.

Several respondents suggested that our guidance should relate only to 'material' outsourcing arrangements. Also, some felt that much of our guidance on outsourcing should not apply when a firm is dealing with a regulated third party as opposed to an unregulated supplier. The same was also said for intra-group outsourcing.

Some respondents queried the applicability of the proposed guidance to specialised products and schemes, such as delegated authority schemes currently in use in the insurance market, where they felt that an additional regulatory burden was inappropriate.

Respondents asked how an insourcer should approach the possibility of multiple requests for access to its premises by auditors who were acting on the behalf of its clients. This was because, in theory, certain suppliers could face hundreds of such requests at any time. One solution that some respondents proposed for this problem was that in many cases one single, independently

verified report on the activities of a provider (such as a SAS 70 or FRAG 21) could replace these audits.

Some respondents asked whether we would expect existing third-party supplier arrangements to be renegotiated in the light of our proposed new policy. It was also suggested that item (2) of 3A.7.4 “the extent to which outsourcing arrangements support the business strategy” be removed, since it was considered unlikely that a firm would take a course that was outside of its business strategy.

**Our response:** We stated in CP142 that we did not wish to distinguish between material and non-material outsourcing in our proposed new policy on outsourcing, and do not intend to deviate from this view. As our policy on outsourcing is all guidance we believe that it is sufficiently flexible to be applied in a proportionate way to both material and non-material outsourcing arrangements. All outsourcing arrangements contain some element of risk that should be managed. Although, clearly, material outsourcing arrangements are likely to represent a higher risk and, therefore, will require more rigorous systems and controls (something that we recognised in the draft text under **SYSC 3A.7.3 G**).

Clearly materiality is an important issue, not least because under SUP 15.3.8G(1)(e) a firm should notify us of its intention to enter into or significantly change a material outsourcing arrangement. However we are concerned that firms might spend too much time determining what is and what is not material outsourcing for the purposes of compliance, rather than for the purposes of good management. In addition we do not wish to include any more guidance on determining materiality, as what is material outsourcing for one firm may not be material for another, depending on the scale and complexity of their operation. We also believe that the firm itself is best placed to judge what is material. If in any doubt a firm is welcome to contact us for further clarification, which in itself should go a long way toward meeting the materiality notification requirements that are set out in our supervision manual.

As for our definition of outsourcing itself, we do not want to narrow this down any further. We believe that our policy is flexible enough to be applied to all situations where there are third-party dependencies.

While we agree that a regulated firm or intra-group entity providing outsourcing services may sometimes represent a lower risk relative to using an external or unregulated supplier, it is still not risk free. Also, we are aware that intra-group outsourcing can represent an even greater risk, for example where a firm is given no choice but to use the services of another group company. For these reasons we do not wish to exempt such arrangements from our policy. Of course where the risk is genuinely lower, the senior management of a firm may wish to use their own judgement as to the extent to which they apply the guidance. We will look at ways in which to redraft the guidance to make this point clearer.

Regarding the application of the guidance to specialised products and schemes, we believe that where the use of such services involves a third-party dependency our guidance on outsourcing should apply. However, we would again stress that, as with all guidance, our policy on outsourcing should be interpreted proportionately.

Turning to the issue of third-party suppliers and the use of independently verified reports, we recognise that it is common market practice in some sectors to obtain assurance through these reports. So we accept that in many cases these reports will be sufficient. However, we would remind firms that when relying on such a report it is the responsibility of senior managers to satisfy themselves that the report:

- is suitably independent and objective; and
- covers all of the issues that they would wish to see addressed.

The use of these reports does not mean that a firm is absolved of the responsibility to maintain any other oversight. Also, the outsourcing firm should not normally have to forfeit its right for itself or its agents to gain access to the premises of the third-party supplier. This is because the loss of this right could undermine the firm's ability to retain sufficient oversight of the provision of services. We will incorporate this approach to the use of independently verified reports into our final text.

We do not expect all regulated firms immediately to renegotiate their third-party supplier agreements when this policy comes into effect. As the policy is all guidance we believe that it is for a firm to decide whether its current outsourcing arrangements are well enough managed to adequately tackle the risks that are associated with them.

Concerning the proposed deletion of 3A.7.4(2), we agree that no prudent firm would take a course that was contrary to its business strategy. However we feel that it is worthwhile to retain this sentence within the final text, to serve as a prompt for those firms whose current approach and practices are not as robust as others.

Q8: Do we cover the right issues in our policy on the use of insurance to finance operational risks? Is this guidance appropriate in terms of its quantity and depth of detail?

- 3.10 Of those that addressed this question, the majority responded positively. It was suggested that more emphasis be placed on the fact that insurance alone may not wholly mitigate certain operational risks. And also that the responsibility will always remain with senior management to consider operational risk concerns and periodically review their arrangements. It was noted by one respondent representing an industry association that the current insurance climate was making it increasingly difficult to negotiate suitable terms and premiums, particularly where the purchasing party may wield little bargaining power. Some respondents also favoured more guidance for firms opting to self-insure or use near-insurance instruments, devised out of a desire to arbitrage certain impediments associated with traditional insurance contracts.

**Our response:** We agree that insurance alone is no substitute for having robust operational risk systems and controls. The tone of the existing guidance already supports this stance, stating as it does that firms take out insurance to reduce, not eliminate, the monetary impact of operational losses. This wording also suggests that operational impact other than monetary considerations will also remain after buying insurance. However, we will endeavour to make this point more explicitly in the final text.

We appreciate that factors beyond the control of the regulated firm may hamper its efforts to negotiate suitable insurance terms, and in such a situation, the firm should consider for itself whether it wishes to pursue the use of insurance as a risk mitigant, or whether it may be more appropriate to find alternative means to manage a particular risk.

As for the treatment of self-insurance, we felt that this practice did not warrant inclusion in a section designed to prompt firms to consider the pitfalls associated with reliance on external insurance contracts. When applying the guidance to emerging near-insurance instruments, the principles to consider remain largely the same, namely that liquidity, counterparty and legal risks may hinder the realisation of the intended benefits of the contract.

Q9: Does our policy amplify, to an adequate degree, the high level rules in SYSC and PRAG 6 that relate to the management of operational risk and the documentation of a firm's operational risk policy?

- 3.11 Most of those respondents who responded to this question were positive in their feedback, and agreed that the correct level of amplification had been achieved. Some respondents, however, felt that the policy was too prescriptive, whilst others felt that more detail could be provided on documentation requirements.

**Our response:** Getting the balance right between providing an adequate amount of guidance and avoiding over-prescription will always require careful attention. We feel that the current level of detail is appropriate, given the flexibility with which it can be applied across a diverse range of firms.

Q10 Are we right to use the term 'assessment' in place of 'measurement'? Should we include some guidance on data collection and the quantification of operational risk?

- 3.12 Almost all respondents agreed that 'assessment' was a more appropriate term than 'measurement'. Two-thirds of the respondents who addressed this question felt that it would be useful to be provided with guidance on data collection and the quantification of operational risk. However, some other respondents felt that the publication of such guidance at this stage would be inappropriate since it could be seen as pre-empting the work of Basel and the EU in this area. Some also felt that any such guidance would hinder innovation in this relatively embryonic area.

**Our response:** We are pleased that our revised wording has met with such approval. Regarding further guidance, we agree that the timing of such guidance would be crucial. We also agree that the content would be driven by a combination of developments in the international arena, and progress made in the field of quantification at the industry level. We intend to monitor this area carefully and will ensure that any guidance that is produced at a later date will be flexible enough to allow for further advances in this field.

Q11: Do you agree that the policy in this CP is compatible with our objectives and general duties under the Act?

- 3.13 This question proved largely uncontroversial, with most respondents agreeing that the proposed policy was in line with our statutory objectives and general duties.

**Our response:** We are pleased that respondents largely agreed that our proposed policy is in line with our statutory objectives and general duties under FSMA, and the assertions that we made in CP142 to this effect remain unchanged.

Q12: Do you agree that this chapter provides a fair estimate of the costs and analysis of the benefits of our systems and controls policy for operational risk in Annexes B and C of this CP? Have any significant costs or benefits been missed out?

- 3.14 Most respondents to this question felt that the cost benefit analysis (CBA) represented a fair estimate of the costs and analysis of the benefits of the proposed guidance. Some respondents felt that the costs may have been understated, while some felt that neither costs nor benefits could accurately be quantified in a meaningful way, and so any CBA performed would be meaningless. Some felt that the costs associated with training staff and bringing about the required culture change were not adequately reflected in our calculations. Other respondents, however, suggested that in some cases our estimated costs were too high, and that in many cases the financial impact on firms of this guidance would be minimal.

**Our response:** Given the diversity of firms within the regulated community, it is inevitable that the cost of implementing our guidance on operational risk systems and controls will vary across firms. For some firms, our assumptions as to the likely costs involved may prove optimistic; however it could equally be said that many others will face costs significantly lower than those predicted. On balance, and in the absence of the provision of alternative estimates from respondents, we feel that our stated cost expectations remain reasonable. Regarding the cost of training staff and fostering culture change across an organisation, such costs were included in our reference to initial and continuing compliance costs, and therefore were taken into account in this way.

We agree that the assessment of the benefits of implementing the stated policy is a largely subjective and qualitative process, which does not lend itself well to comparisons against the monetary cost of implementation. However, we remain confident that the benefits gained by the industry are significant enough to outweigh any costs. These benefits would be in terms of the expected reduction in the likelihood and impact of operational losses, and the impact that this would have on the market as a whole and on consumers.

# 4 Next steps

## International Developments

- 4.1 The dual efforts at both Basel and the European Commission to review the current capital adequacy framework to take account of operational and other risks for those firms subject to their respective capital requirements continue to make progress. Basel publications on the capital accord can be found at the following Internet address:

<http://www.bis.org/bcbs/publ.htm>

- 4.2 The EU's latest published proposals can be viewed at the following internet address, and form part of a structured dialogue paper, which sought feedback from interested parties. Although the deadline for feedback has passed, a further formal consultation exercise is planned for later this year.

[http://europa.eu.int/comm/internal\\_market/en/finances/capitaladequacy/index.htm](http://europa.eu.int/comm/internal_market/en/finances/capitaladequacy/index.htm)

- 4.3 Some of the respondents to CP142 seemed unsure about whether we were going to implement any capital requirements for operational risk. We are, and firms that are subject to the Basel/CAD requirements should expect more from us on this issue in the future. However, that said, we do not intend to publish any draft rules on the calculation of capital requirements for operational risk until the outcomes of the relevant international work streams become clearer. We would recommend that any firm wishing to stay abreast of developments at both Basel and the Commission should review the above websites, and take every opportunity to provide input into the final proposals. Details of our current work regarding international developments can be found at the following Internet address:

[http://www.fsa.gov.uk/international/1\\_caf.html](http://www.fsa.gov.uk/international/1_caf.html)

## **Next Steps for the Policy in CP142**

- 4.4 We expect to publish our near-final Handbook text for operational risk systems and controls, along with all of our other new policy on systems and controls, later this year. This material will take effect in 2004, as part of the first phase of the implementation of the Integrated Prudential Sourcebook.
- 4.5 We are still considering our policy on Professional Indemnity Insurance (“PII”), and will continue our work on this. We recently published a Consultation Paper on PII, CP169, which can be found at the following Internet address:

<http://www.fsa.gov.uk/pubs/cp/169/index.html>



# List of non-confidential respondents

Abbey National

Aberdeen Asset Management

Association of British Insurers

Association of Friendly Societies

AMP

APCIMS

Aviva

AXA

Baillie Gifford & Co

British Bankers Association/London Investment Banking Association  
joint response

British Venture Capital Association

Citigroup

Depositary and Trustee Association

Financial Guardian Group

Financial Services Consumer Panel

Friends Provident

FSA Small Business Practitioner Panel

GMAC-RFC Limited

Healthsure

Investment & Life Assurance Group

Investment Management Association  
International Petroleum Exchange  
JP Morgan Group  
KPMG  
Legal & General  
Liverpool Victoria  
Lloyds  
Lloyds TSB  
M&G Limited  
Merrill Lynch  
Nationwide Building Society  
OpRisk Limited  
Patients' Aid Association  
PricewaterhouseCoopers  
Prudential  
Scottish Widows  
Standard Life  
WestLB Panmure Limited  
Yorkshire Building Society  
Zurich Financial Services (UKISA) Limited



**ISBN: 0117041033**

The Financial Services Authority  
25 The North Colonnade Canary Wharf London E14 5HS  
Telephone: +44 (0)20 7676 1000 Fax: +44 (0)20 7676 1099  
Website: <http://www.fsa.gov.uk>

Registered as a Limited Company in England and Wales No. 1920623. Registered Office as above.