## Contents

1 Executive summary 3
2 Introduction 6
3 Overview of Operational Risk Management Systems and Controls 11
4 Feedback on Comments on PROR 1 and PROR 2 in CP97 19
5 Compatibility with our Objectives and General Duties under the Financial Services and Markets Act 2000 26
6 Cost Benefit Analysis 33

**Annex A:** List of Questions in this Consultation Paper

**Annex B:** Draft Guidance on Operational Risk Systems and Controls for SYSC

**Annex C:** Draft Guidance on Operational Risk Systems and Controls for the PSB
The Financial Services Authority invites comments on this Consultation Paper. Comments should reach us no later than 31 October 2002, although earlier responses would be welcomed, particularly if they involve substantial comments. Throughout this Consultation Paper we have highlighted questions on which we would particularly welcome your views.

Comments may be sent by electronic submission using the form on the FSA’s website (at www.fsa.gov.uk/pubs/cp/cp142_response.html).

Alternatively, please send comments in writing to:

Simon Ashby
Prudential Standards Division
The Financial Services Authority
25 The North Colonnade
Canary Wharf
London E14 5HS

Telephone: 020 7676 0986
Fax: 020 7676 0987
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 Our initial proposals for rules and guidance on operational risk were outlined in Consultation Paper 97: Integrated Prudential Sourcebook (CP97) issued in June 2001. We are reconsulting on the material about operational risk systems and controls and outsourcing because we have materially revised the draft text on which we consulted in CP97. This Consultation Paper (CP) seeks comments on this proposed new Handbook text, all of which is guidance. We expect that this guidance will take effect in 2004.

1.2 For insurers, the proposed Handbook text in this CP will take forward and complement the proposed guidance on risk management systems and controls, as presented in CP140 (The Interim Prudential Sourcebooks for Insurers and Friendly Societies and the Lloyd’s Sourcebook: Guidance on Systems and Controls).

1.3 This CP will be of some interest to retail consumers because its proposals promote our consumer protection objective, by ensuring that firms manage their operational risks adequately. Our general systems and controls requirements and specific guidance on operational risk are intended to help ensure that firms have adequate systems and controls to comply with our Conduct of Business and Client Money rules. But, this CP does not propose changes to how our COBS and Client Money rules operate. Our guidance should, therefore, help to reduce direct losses to consumers arising from operational failures at firms. In addition, our guidance should help to reduce the frequency and impact of operational losses that may deplete a firm's financial resources, and hence ensure that firms remain able to meet their liabilities as they fall due. Our statement on our policy’s compatibility with our objectives and general duties under the Financial Services and Markets Act 2000 (in Chapter 5 of this CP) sets out in more detail how our consumer protection objective is achieved.
1.4 Operational risk management failures at firms could have an impact on at least three of our statutory objectives:

(a) a firm’s customers may suffer losses, if the firm mishandles their assets, or otherwise fails to discharge adequately its customer obligations;

(b) a firm may suffer losses, with the potential for damaging confidence in the financial system and for knock-on losses to consumers; and

(c) a firm may be more susceptible to financial crime.

1.5 Our guidance is intended to help firms to reduce the frequency and impact of operational risk management failures in a cost-effective way, furthering our statutory objectives, but not placing an undue burden on firms.

1.6 One significant change from our earlier consultation on this topic is that it is now proposed that some of our guidance on operational risk management systems and controls, including that on outsourcing, should be located in SYSC (Senior Management Arrangements, Systems and Controls). This change has stemmed from our view that placing all our guidance on operational risk in the Integrated Prudential Sourcebook (PSB) would not highlight sufficiently the effects that operational risk management failures may have on our consumer protection and financial crime objectives. The SYSC guidance on operational risk systems and controls will apply to almost all regulated firms, as set out in SYSC 1 (see Annex B).

1.7 The guidance on operational risk identification, assessment, monitoring and control, and the content of a firm’s operational risk policy, that will be in the PSB is designed to be complementary to SYSC. This guidance will apply to fewer firms. It will broadly affect deposit-takers, insurance firms, investment firms that take principal positions, and investment firms and Lloyd’s agents that hold client money.

1.8 We do not expect that the overall impact of this policy on firms will be adverse. We have framed our proposed Handbook text on operational risk as guidance on the application of high level requirements for adequate systems and controls in SYSC 3 (Systems and controls) and PRAG 6 (Prudential systems and controls) of the PSB. As such, there is flexibility for firms to make cost-effective arrangements that are appropriate to their particular business and proportionate to their risks, and that assist them in the management of their business.

1.9 We consider that our guidance reflects common practices at prudently managed firms and that many firms already meet it. As a consequence, we believe that the benefits of this policy will be more than proportionate to the costs.
1.10 This CP contains the following chapters:

- Chapter 2 - outlines the purpose of this CP and our guidance on operational risk, including the background to the development of our policy, our timetable for implementing the policy and its context in the current international discussions on operational risk.

- Chapter 3 – outlines the structure and content of our guidance on operational risk management systems and controls, and briefly considers the definition and scope of operational risk.

- Chapter 4 – provides feedback on the comments we received on PROR 1 and 2 as part of the CP97 consultation process and our responses to these comments.

- Chapter 5 - sets out the statement of compatibility with our statutory objectives.

- Chapter 6 contains our cost benefit analysis.

- Annexe A lists the questions in this CP.

- Annexes B and C contain the draft Handbook text.

Next steps

1.11 We are still considering our policy on professional indemnity insurance and will be carrying out further work on this. Our feedback statement on the responses to CP97 and CP115 offers further discussion of this topic.

1.12 We will consider the comments received in response to this CP (the deadline for comments is 31 October 2002) when we develop our operational risk policy. We expect to publish a Policy Statement outlining our conclusions on operational risk systems and controls, including final Handbook text, in 2003. As we stated in CP115, we expect the policy will then take effect in 2004, as part of the first phase of the implementation of the PSB.
2 Introduction

Background

2.1 We outlined our initial proposals for rules and guidance on operational risk in Consultation Paper 97: Integrated Prudential Sourcebook (CP97). CP97 was issued in June 2001 and proposed three chapters, one on operational risk systems and controls in general (PROR 1), one on outsourcing systems and controls (PROR 2), and one on professional indemnity insurance (PROR 3). We are reconsulting on operational risk systems and controls and outsourcing (PROR 1 and 2, as was) because we have materially revised the draft text on which we consulted in CP97. This new guidance is intended to form part of our Handbook of Rules and Guidance and will come into effect in 2004. Our thoughts on PROR 3 are discussed in our feedback statement for CP97 and CP115 (Integrated Prudential Sourcebook – Feedback on CP115 (Integrated Prudential Sourcebook – Timetable for Implementation) and CP97 (Integrated Prudential Sourcebook)).

2.2 A key motive behind our decision to revise our draft text on operational risk systems and controls was our desire to include additional guidance on operational risk in SYSC (Senior Management Arrangements, Systems and Controls). This is to emphasise that operational risk may cause direct losses to consumers as well as to firms. We propose to include this guidance in a new chapter, SYSC 3A (Operational Risk Systems and Controls).

2.3 We also propose to add some subject specific guidance on a number of key areas of operational risk management. This draft text addresses areas such as business continuity management, the use of insurance to finance operational losses and the management of operational risks that arise out of a firm’s people, processes and systems.

2.4 Finally, we have revised our text to take account of the detailed and helpful comments that were provided by the external respondents to PROR 1 and 2 of CP97. In response to these comments our revised version of PROR 1, which will now be called PRU 6.1 (Operational Risk Prudential Systems and
Our decision to remove the module abbreviations PRAG, PROR, etc. and remodel the PSB in line with the rest of the Handbook is discussed in our feedback statement to CP97 and CP115. However, for consistency we still use these old abbreviations when we discuss the draft text that was in CP97.

2.5 Thus some of the guidance proposed in this CP will be added to the guidance on our general requirements in the Handbook relating to senior management arrangements, systems and controls (as contained in SYSC). This guidance will apply to almost all regulated firms, as set out in SYSC 1 (see Annex B). The remainder will form part of the Integrated Prudential Sourcebook (PSB), which will replace the Interim Sourcebooks in the business standards section of the Handbook. The PSB guidance will apply to firms in prudential categories 1 to 4B (broadly deposit-takers, insurance firms, investment firms that take principal positions, and investment firms and Lloyd’s agents that hold client money).

Links with current international work

2.6 The prudential regulation of operational risk is currently being discussed at two main international fora:

- The Basel Committee on Banking Supervision, where a revised Capital Accord² (Basel 2) is being drawn up. This contains new proposals for operational risk that include the introduction of a capital charge, as well as systems and controls and disclosure requirements.

- The European Union, where so-called CAD3 work is being conducted, in parallel to Basel 2, on the setting of operational risk capital and systems and control requirements for banks and investment firms.³ The European Union is also starting work on proposals for new solvency directives for insurers.⁴ This may include operational risk management systems and controls requirements for general and life insurers.

---

1 Our decision to remove the module abbreviations PRAG, PROR, etc. and remodel the PSB in line with the rest of the Handbook is discussed in our feedback statement to CP97 and CP115. However, for consistency we still use these old abbreviations when we discuss the draft text that was in CP97.


4 The so-called Solvency 2 review.
2.7 As stated in CP97, we have not tried to anticipate in our policy the international operational risk management standards that may arise as a result of these discussions. In addition, draft rules on the calculation of capital requirements for operational risk will not be issued for consultation in the UK until the outcomes of the Basel 2 and CAD3 discussions become clearer.

Purpose for which operational risk rules and guidance are made

2.8 We believe that the inadequate management of operational risk could present a significant threat to three of our statutory objectives, those of securing the appropriate degree of protection for consumers, of maintaining confidence in the financial system and of reducing financial crime. Operational risk management failures can significantly disrupt the quality and continuity of a firm’s business activities. They may cause losses to the firm’s clients or to the firm itself and at the extreme may cause it to become insolvent. Losses may be sustained through:

- a firm’s operational failure to identify and appropriately control financial risks encountered in the ordinary course of its business;
- disruption to the firm’s business activities;
- the mishandling of clients’ assets and money;
- inappropriate advice or selling to clients;
- the susceptibility of a firm to fraud; and
- a firm becoming a target for money laundering.

2.9 Some specific areas of concern relating to operational risk include:

- highly automated and integrated technology that has the potential to transform risks from minor manual processing errors to major systematic failures;
- the growth in e-commerce that brings with it some new and potentially significant operational risks for both consumers and firms (e.g. fraud and system security issues);
- firms that outsource their activities may suffer some loss of control over them, which could affect the quality and availability of their products; and
- insourcing, where firms take on the operational risks of third parties.

2.10 In fact, investigations into the failure of many financial firms have revealed that the underlying causes of many losses were operational, even though the immediate cause of these losses appeared market or credit related. For example, they may be due to failures in management systems and internal controls.
2.11 The guidance on operational risk that we propose for the Handbook is designed to complement our high level rules in SYSC and the draft rules of PRAG 6 that require firms to be prudently managed and, in particular, to have appropriate risk management systems and controls. We discuss in more detail in Chapter 5 of this CP how our proposed guidance may help us to meet our statutory objectives.

**Purpose of this consultation paper**

2.12 We have powers to make rules and guidance under sections 138 and 157 of the Financial Services and Markets Act 2000. In this consultation paper we do not propose to make any new rules, however, under section 157 we propose to issue guidance on operational risk systems and controls.

2.13 This CP is intended to comply with the requirements of sections 155 and 157 of the Act. These require us to consult on draft rules and on any guidance that we propose to give to authorised persons (or to a class of regulated person) about those rules. When we consult on draft rules or guidance, under sections 155(2) and 157(3), we must also publish:

- a cost benefit analysis;
- an explanation of the purpose of the rules; and
- an explanation of why we believe them to be compatible with our general duties under section 2 of the Act.

**Timetable**

2.15 We outlined our views on the timing of the implementation of the PSB in CP115 (Integrated Prudential Sourcebook – Timetable for Implementation, November 2001). We proposed to implement PSB rules and guidance on risk management systems and controls in 2004. We consider that a timetable of 2004 for operational risk systems and controls guidance is appropriate and do not believe that the reallocation of some operational risk guidance to SYSC from the PSB should change that timetable.
2.16 The envisaged timetable is as follows:

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>August 2002 to October 2002</td>
<td>Three month consultation period on the proposals in this paper.</td>
</tr>
<tr>
<td>2</td>
<td>November 2002 to December 2002</td>
<td>FSA reviews responses to consultation and prepares final policy.</td>
</tr>
<tr>
<td>3</td>
<td>2003</td>
<td>FSA publishes final policy for operational risk management systems and controls.</td>
</tr>
<tr>
<td>4</td>
<td>2003/2004</td>
<td>One year for firms to prepare for implementation of the operational risk management systems and controls policy.</td>
</tr>
<tr>
<td>5</td>
<td>2004 (the precise timetable is yet to be determined)</td>
<td>Operational risk management systems and controls policy takes effect.</td>
</tr>
</tbody>
</table>

The consultation process

3.17 We are publishing this CP in hard copy as well as making it available on our web site (http://www.fsa.gov.uk/) and monthly CD-ROM issue. We will be bringing it to the attention of both the firms that will have to comply with SYSC and the PSB, and through representative consumer groups, to financial services consumers. A number of discussions with trade associations have already taken place and we will have a continuing dialogue with them about the finalisation of this policy.

Who can respond?

3.18 We would welcome responses from anyone with an interest in operational risk management systems and controls, or who may be affected by our guidance on them. We need your responses to reach us no later than 31 October 2002. An early response would be particularly welcome if it concerns substantial matters. Throughout this CP, we have highlighted questions on which we are particularly keen to receive your views. These are listed in Annex A.
3 Overview of Operational Risk Management Systems and Controls

3.1 This chapter provides an overview of our proposed guidance on operational risk management systems and controls. It begins with a brief discussion of the nature of operational risk. It then gives a summary of how our guidance in this area has been structured, and what the main components are.

The nature of operational risk

3.2 The Basel Committee on Banking Supervision has suggested that operational risk is:\(^{5}\)

“the risk of loss, resulting from inadequate or failed internal processes, people and systems, or from external events”.

3.3 This wording is based on a common industry interpretation of operational risk. It is very broad in that it focuses on all the general sources of operational risk that can be present in a firm. For example, operational risk could be created by a wide range of different external events from floods to terrorist attacks. Similarly, operational risk can arise due to the potential for failures or inadequacies in any of the firm’s processes and systems (e.g. its IT, risk management or human resource management processes and systems), or indeed those of its outsourced service providers. Finally, ‘people’ can refer to a range of issues such as mis-managed or poorly trained employees, or the potential for people to perpetrate fraud, rogue trading and so on.

3.4 However, this wording has some inadequacies in a broader context, in particular for insurers. An insurer may explicitly underwrite risks to policyholders of an operational nature as part of its insurance business. Equally an insurer (and consequently its policyholders and counterparties) is as susceptible as a deposit taker or investment firm (and its clients and counterparties) to operational failures of the firm’s systems and controls, and the impact of external events that are part of conducting business.

---

3.5 Ultimately firms need to decide for themselves what operational risk means to them. In particular, a firm should consider a more specific definition of operational risk that is appropriate to the range and nature of its business activities and its operating environment. Our guidance on operational risk is intended to give firms pointers to the factors that they should consider in the light of the risks they may pose to our statutory objectives.

**General approach**

3.6 We include in this CP draft text on operational risk management for two parts of the *Handbook*: SYSC and PSB. The SYSC text will form a new chapter, SYSC 3A, that provides guidance on SYSC rules:

- 3.1.1R, ‘a firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business’; and
- 3.2.6R, ‘a firm must take reasonable care to establish and maintain effective systems and controls for compliance with the applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime’.

3.7 The application of SYSC 3A is set out in SYSC 1, for further details see Annex B.

3.8 The PSB text will form a separate chapter (PRU 6.1) of that *Sourcebook* and will provide guidance on applying the general prudential risk management systems and controls rules that were proposed in PRAG 6 of CP97. This will apply to firms in prudential categories 1 to 4B (broadly, deposit-takers, insurance firms, investment firms that take principal positions, and investment firms and Lloyd’s agents that hold client money).

3.9 Three factors have influenced this decision:

(a) The inadequate management of operational risk has potential adverse implications for all categories of firm. It may affect their solvency, the adequate discharge of their obligations to their customers, and the susceptibility of such firms to financial crime. So, we consider that there should be some guidance on operational risk management in SYSC, where all these risks to our objectives can be addressed.

(b) In response to CP97 firms requested guidance in the PSB to help clarify our expectations on the establishment and maintenance of operational risk systems and controls in a prudential context. So, we have included additional guidance in our revision of PROR 1 (now PRU 6.1). PRU 6.1 gives guidance on the proposed rules in PRAG 6, relating principally to: the establishment and maintenance of systems and controls for the management of prudential risks; the formulation and documentation of a business plan and risk policy statements; and prudential record
keeping requirements. It will follow a structure similar to that proposed for market, credit and insurance risk systems and controls, prompting a firm to make appropriate arrangements to identify, assess, monitor and control operational risk.

(c) Certain categories of firms such as investment firms that do not hold principal positions, or client money and credit unions are exempted from many, if not all, of our proposed prudential requirements, including a number of the rules relating to systems and controls in PRAG 6 of CP97. This is why these categories of firm are excluded from our policy on operational risk systems and controls in the PSB (consistent with market, credit and insurance risk). However, we plan to prompt them to consider operational risk in the context of the risks that they pose to our objectives by including guidance that applies to them in SYSC.

3.10 We recognise that different firms are engaged in very different businesses and have different operating environments, so their operational risks vary considerably. We have, as a consequence, taken a high level, issues based, approach to the drafting of our guidance on operational risk management systems and controls. This ensures that our policy may be interpreted in a flexible manner that is appropriate to the business and circumstances of an individual firm.

3.11 The guidance prompts firms to consider the relevance of a number of issues in the context of their business, and then to make appropriate arrangements for risk control. It does not specify the precise systems and controls that they should be using to manage their operational risks. This, we believe, is consistent with the fact that primary responsibility for the management of risk rests with the firm and its senior management.

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?

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

SYSC 3A: Operational risk systems and controls

3.12 The guidance in this chapter will be applicable to almost all firms (for full details see SYSC 1). The main components of the guidance are:

- a discussion of the definition and scope of operational risk;
- how common risk management concepts may be applied in an operational risk context; and
• the main operational risks that may arise from a firm’s people and processes and systems, external events, and outsourcing.

3.13 There is also guidance on the use of insurance to finance operational losses. Many of the new topics that have been introduced into our guidance since CP97 have been incorporated into this chapter.

People

3.14 The way in which a firm manages its employees can be a major source of operational risk. Poorly trained or overworked employees may inadvertently expose a firm to operational risk (for example, via processing errors). In addition, a firm may find that the availability of its employees, or its ability to replace them, can influence its ability to recover from interruptions to the continuity of its operations.

3.15 Given that the management of a firm’s employees is a major source of operational risk, we think that some specific guidance on this issue is needed. For example, a firm that invests time and money in creating an appropriate risk culture, in which employees are aware of operational risks and are encouraged to learn from their mistakes, can realise significant improvements in its control of operational risk and reduce exposure.

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?

Processes and systems

3.16 A firm’s operations may be supported by many different systems and processes, such as IT systems, human resource management systems, credit, market, insurance and liquidity risk management systems and even operational risk management systems. These systems may have many different components, each of which will require the operation of various processes. For example, the credit risk management system of a firm should have processes for the identification, measurement, monitoring and control of credit risk.

3.17 Complex or poorly designed systems and processes can give rise to operational losses, either because they are unfit for purpose, or because they malfunction. As a result, a firm may experience a wide range of problems, including settlement-processing errors, fraud and information security failures. In addition, the increasing automation of systems and our reliance on IT has the potential to transform risks from minor manual processing errors to major systematic failures.
3.18 The purpose of this section is to draw a firm’s attention to processes and systems as sources of operational risk and to offer guidance on a number of means of controlling such risks. In particular, the draft Handbook text contains guidance on the management of risks from IT systems, the documentation of systems and processes (to parties that are both internal and external to the firm) and the security of a firm’s information systems. We also want multinational firms that operate systems and processes in more than one country to consider the additional risks that this can entail.

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?

External events and other changes (including business continuity management)

3.19 As was demonstrated by the attack on the World Trade Centre on 11 September, external events can have a major impact on a firm. A firm should be aware that both expected and unexpected changes to its operations can be major sources of operational risk. This section of our policy contains some guidance on the management of operational risks that result from changes that may be externally or internally generated.

3.20 The majority of the guidance in this section relates to business continuity management. We have already indicated the importance of business continuity management in SYSC 3.2.19G, which states:

“A firm should have in place appropriate arrangements, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness”.

3.21 The Handbook text in this CP provides complementary guidance to SYSC 3.2.19G. This text is also consistent with the approach to business continuity management that we have already outlined in our working paper on the UK Financial Sector Continuity website (this is available in downloadable pdf format from www.financialsectorcontinuity.gov.uk). In particular, we believe that a firm should assess the various internal and external events that may disrupt its operations and plan for possible responses to these disruptions. We are also concerned that firms should organise appropriate back-up site arrangements. A key issue here is the outsourcing of back-up site services, particularly where the quality and availability of these services is not as good as a firm might be able to provide internally. For example, a firm that outsources its back-up provision to a provider that offers shared back-up site facilities may not have guaranteed access to this site if someone else is using it.
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?

**Outsourcing**

3.22 As stated in the feedback statement to the responses to CP97 (see Chapter 4), we have revised our *Handbook* text to take a simpler and more guidance orientated approach to our policy on outsourcing.

3.23 We recognise that there are many reasons why firms may wish to outsource some of their activities and that outsourcing may, in certain circumstances, help to reduce the level of operational risk faced by a firm. However, outsourcing arrangements require careful management if they are to yield benefits, and where they are not managed adequately the degree of operational risk faced by a firm can increase. In particular, we are concerned about the loss of control a regulated firm may experience over the quality of performance of outsourced activities. This is because, unlike internally conducted activities, the control a firm can exercise is often highly related to how well the contract with its service provider has been drafted. Furthermore, a firm that outsources activities may lose its ability to conduct them in house, particularly if staff with vital expertise are lost. This could make it dependent on external service providers and create a serious threat to the continuity of its operations if these providers were to fail.

3.24 Our revised *Handbook* text on outsourcing is designed to highlight the importance of managing outsourcing arrangements effectively. This guidance reflects the four main phases that make up the life cycle of a firm’s outsourcing arrangements:

- The decision to outsource or change an existing outsourcing arrangement (the decision making phase).
- Drafting an outsourcing contract (the contract drafting phase).
- The implementation and maintenance of an outsourcing arrangement (the contractual phase).
- Dealing with the expected or unexpected termination of a contract (the post-contractual phase). In particular, we are concerned that a firm should maintain the continuity of its business in the event that an outsource service provider might fail.

3.25 It is important to note that the scope of this policy covers all forms of outsourcing, including non-material and intra-group outsourcing. No form of outsourcing is entirely risk free, but we recognise that the management of non-material and intra-group outsourcing should be proportionate to the risks presented by these arrangements.
Q6: Are we right to rely on guidance in our policy on outsourcing?

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?

Insurance

3.26 SYSC 3A also includes guidance on the use of insurance to cover operational risks. We recognise the risk management and financial benefits that insurance can bring to firms. However, risk mitigation tools like insurance carry with them their own set of risks. In particular, the firm may find that in mitigating its operational risks, it incurs a counterparty risk and, potentially, liquidity risk.

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?

PRU 6.1: Operational risk prudential systems and controls

3.27 The guidance in this chapter of the PSB (PROR 1 as was) has been largely revised in response to requests from respondents to CP97 for more guidance on applying the rules that we proposed in PRAG 6 in an operational risk context. It is intended that it will apply to firms in prudential categories 1 to 4B (broadly, deposit-takers, insurance firms, investment firms that take principal positions, and investment firms and Lloyd’s agents that hold client money).

3.28 The chapter gives guidance on what firms should include in their operational risk policies. This guidance has deliberately been kept high level, since we would expect the structure and content of firms’ policy statements to differ according to the nature of their activities and the complexity of their operational risks. A high level approach has also been adopted for the guidance on risk identification, risk assessment, risk monitoring and risk control. This is because we recognise that firms may adopt very different approaches to undertaking these processes.

3.29 A key issue in this context is operational risk measurement. We acknowledge that due to both data limitations and a lack of high powered analysis tools, a number of operational risks cannot be measured accurately in a quantitative manner at the current time. So, we have decided to use the term risk assessment in place of measurement, to encompass more qualitative processes, including, for example, the scoring of risks as ‘high, medium, and low’. However, we would still encourage firms to collect data on their operational risks and to use measurement tools where this is possible and appropriate. We believe that using a combination of both quantitative and qualitative tools is the best approach to understanding the significance of a firm’s operational risks.
Finally, we have included some guidance offering examples of how firms might fulfil the high level rules and guidance on record keeping that were proposed in PRAG 6.11 of CP97, in particular, PRAG 6.11.3(G), which deals with the contents of a firm’s records for market, credit, insurance, operational and group risk. As this is guidance, it does not mandate that such records are appropriate for all firms. We would expect firms to keep records that suit their needs and reflect the risks that they pose to our statutory objectives.

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?

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?
Feedback on Comments on PROR 1 and PROR 2 in CP97

PROR 1: Operational risk systems and controls

4.1 In CP97 one question was asked about PROR 1:

Q50: Does the proposed chapter on operational risk reflect the main prudential risks to firms in this area? Do the requirements add usefully to the general material on systems and controls in SYSC? Should the chapter be more detailed – as for example, the chapters on credit risk and market risk systems and controls?

4.2 With only a few exceptions, the general feeling of the respondents to Q50 was that we had covered the main prudential risks in this area, but that more guidance on the management of some of these risks was needed. It was felt that PROR 1 could have done more to support the rules and guidance in SYSC.

4.3 The specific themes raised by respondents, and our feedback on each of them, are set out in more detail below.

The use of guidance

4.4 Many of the respondents to the operational risk systems and controls policy in PROR 1 of CP97 requested more guidance. Two main reasons were given for this request. First, several respondents felt that PROR 1 could have given more guidance on how SYSC and PRAG 6 would apply in an operational risk context. This related in particular to those categories of operational risk outlined in PROR 1.3.4-1.3.11 that are complex to manage or might have a high impact on our objectives (for example IT systems, or disaster risk). Second, a small number of respondents felt that we should issue guidance on what we saw as the scope of operational risk management and the effective management of operational risk.

6 The categories detailed in PROR 1.3.4-1.3.11 were business risk, crime risk, disaster risk, information technology risk, legal risk, regulatory risk, reputation risk and systems and operations risk.
4.5 These comments indicate that there is support for changes to be made to the content of our systems and controls policy for operational risk and for additional guidance. However, many respondents also stressed that our policy should not be too prescriptive. Their main argument was that the compliance costs associated with a prescriptive approach would be too high and in particular might have a disproportionate effect on small firms if they were required to have arrangements that were not justified by the underlying risk. Others argued that we should leave the development of detailed guidance to trade and professional associations.

**Our response:** We agree that more guidance on operational risk systems and controls is needed and that our policy should not be overly prescriptive. With this in mind we have drafted revised Handbook text that is framed wholly as guidance on our general requirements for adequate systems and controls in SYSC 3 and PRAG 6. By using guidance we allow firms to adopt a more flexible approach to the management of operational risk that is proportionate to their circumstances.

We also agree that our guidance on operational risk could be structured to support better the rules and guidance in SYSC. So we have drafted part of our revised guidance on operational risk as a new chapter of SYSC, SYSC 3A. This gives guidance on SYSC rules:

3.1.1R, ‘a firm must take reasonable care to establish and maintain such systems and controls as are appropriate to its business’; and

3.2.6R, ‘a firm must take reasonable care to establish and maintain effective systems and controls for compliance with the applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime’.

This text gives guidance on the risks that may arise from a firm's people, processes and systems, or from external events, and covers such topics as business continuity, outsourcing and information security.

The revised text of PROR 1 (now PRU 6.1) supports our proposals in PRAG 6, by giving guidance on a firm's business plan and operational risk policy, and the identification, assessment, monitoring and control of operational risk.

**External developments in the practice and regulation of operational risk**

4.6 Some of the respondents to CP97 pointed out that operational risk is a developing area. A minority asserted that it is so developmental that meaningful policy on operational risk systems and controls cannot be drafted at the current time. Others noted that both the Basel Committee for Banking Supervision review of its capital accord and the European Union Capital Review for banks and investment firms are not concluded. This led some respondents to suggest that we should delay the implementation of all our operational risk policy until we know the outcome of at least the Basel negotiations.

---

7 This refers to the so-called Basel 2 process.

8 This is also known as the Third Capital Adequacy Directive, or CAD 3.
Our response: We believe that the prudent management of operational risk by a firm is necessary to the achievement of our statutory objectives (as we have set out in our compatibility statement in Chapter 5 of this CP). This is why we consider it appropriate to give guidance now on the management of operational risk, and to clarify how our general rules on systems and controls in SYSC and PRAG 6 will apply in an operational risk context, rather than awaiting a conclusion to international negotiations. We have, however, revised our policy to reflect better the approach taken by the first draft of the Basel Risk Management Group’s paper “Sound Practices for the Effective Management and Supervision of Operational Risk” that was published for consultation in December 2001, as suggested by some CP97 respondents.

The purpose of the Basel ‘Sound Practices’ paper was to create a dialogue with firms on the effective management of operational risk. The paper outlines seven general ‘Principles’ for the sound management of operational risk by financial firms. It also highlights issues such as the importance of developing an appropriate operational risk policy, the need to establish processes for the identification, measurement, monitoring and control of operational risk, and the importance of senior management involvement in operational risk management. Although Basel focuses on the management of risk within internationally active banks, the principles outlined in its ‘Sound Practices’ paper are general enough to apply to all financial firms.

Capital for operational risk

4.7 A number of respondents expressed concerns about capital requirements for operational risk.

Our response: This CP does not propose a capital requirement for operational risk. We will, however, need to review the issue of a capital requirement once the Basel and EU negotiations are concluded. We would, naturally, consult on any proposals for a capital requirement that we may make.

Terminology

4.8 The use of the term ‘risk measurement’ in relation to operational risk was a source of concern to a number of CP97 respondents. They argued that operational risks can be very difficult to measure with quantitative precision.

Our response: We accept that there is not enough data on some operational risks to enable quantification, and that tools for the analysis of operational risk are still developing. So, as suggested by some respondents to CP97, we have decided to use the term ‘risk assessment’ in place of ‘risk measurement’ to avoid any confusion. We understand that the financial industry views risk assessment as a rather broader process than risk measurement (which is typically used to describe the formal process of quantifying risk). As such, the term risk assessment can be used to describe both the

---

9 A second, revised, draft of the Basel ‘Sound Practices’ paper should be published this summer.
PROR 2: Outsourcing

4.9 One question was also asked in CP97 on PROR 2:

Q51: Does the proposed approach to outsourcing reflect the main prudential risks to firms in this area? Is it clear what we mean by a material outsourcing? Do the requirements add usefully to SYSC? Should the scope of the outsourcing chapter include category 5 firms?

4.10 Of the respondents that addressed this question very few provided a direct answer to all of it, although many stated that they were unclear as to the meaning of material outsourcing.

4.11 Many respondents did, though, ask us to clarify the application of our requirements to outsourcing arrangements that a firm may have with another member of its group (which they felt presented a lower risk to firms and our regulatory objectives). They also asked how existing outsourcing contracts would be grandfathered into the new regime. Finally, some respondents commented that CP97 was too prescriptive in its approach to outsourcing.

4.12 The specific themes raised by respondents, and our feedback on each of them, are set out in more detail below.

Outsourcing and third party dependencies

4.13 A few respondents suggested that we should use the term ‘third party dependencies’ instead of outsourcing. The argument for this is that it is third-party dependencies (i.e. the failure of an important third party service provider or the provision of inadequate services) rather than outsourcing as such, that is the main concern for our statutory objectives.
Our response: We agree that we are concerned that outsourcing arrangements may make a firm dependent on a third party for the provision of certain services, and leave them vulnerable in the event of a failure by that party. Outsourcing is a term that is in common use throughout the financial services industry and we consider that it is a useful label because of that familiarity. We are, however, keen to make clear the breadth of our outsourcing policy, and that it covers a range of ‘outsourcing’ activities undertaken by financial firms. In particular, we have tried to shed further light on our definition of ‘third party’ in the new policy, by making it explicit that a firm in the same group that provides services to a regulated firm would be encompassed by this definition.

Intra-group outsourcing

4.14 Some respondents felt that intra-group outsourcing should be excluded from our policy, while others called for it to receive a more lenient treatment.

Our response: We agree that the provision of services by a member of the same group as a regulated firm may sometimes be less of a risk than using a non-group service provider. However, intra-group outsourcing is not risk free and so we do not wish to exempt intra-group outsourcing from our policy. We accept that where risk is less, systems and controls do not need to be so rigorous. Nevertheless, it is for the management of the regulated firm to assess this risk and to make arrangements for its management, as appropriate.

Material outsourcing

4.15 Many respondents to CP97 felt that our definition of material outsourcing needed clarification. They felt that there is a large middle ground of outsourcing activities where it is difficult to determine materiality under our current definition.

Our response: We consider that the CP97 definition is adequate. What is a material outsourcing activity for one firm may not be material for another, depending upon the nature and extent of its business activities. So we believe that a firm is best placed to judge for itself what is material, in the context of its particular business. The systems and controls that a firm has in place to manage its outsourcing arrangements may be the subject of dialogue between us and the firm, and one element of that may be how a firm identifies what is material in the context of its business.

Our current definition of material outsourcing is “outsourcing services of such importance that weakness, or failure, of the services would cast serious doubt upon a firm’s continuing satisfaction of the threshold conditions or compliance with the principles”.

Financial Services Authority 23
Transitional provisions

4.16 Almost all of the respondents that commented on our outsourcing policy were unsure as to whether and/or when existing outsourcing contracts would need to be rewritten to be compliant with it. Outsourcing contracts can run for many years and firms were concerned to know whether they would be required to renegotiate them mid-term.

**Our response:** Our revised Handbook text on outsourcing is framed as guidance that is intended to prompt firms to consider whether their outsourcing agreements address adequately the risks that may be present in the arrangements that they have. We have not imposed detailed prescriptive requirements on the content of agreements and so do not consider that formal transitional arrangements will be necessary. It will be for a firm to consider whether its current outsourcing contracts are sufficiently tightly drafted to enable it to manage adequately the risks that may be present, and whether/when existing outsourcing arrangements may need to be renegotiated.

The prescriptive nature of the outsourcing policy in CP97 and the introduction of a materiality criterion for the application of some of our rules

4.17 There was a general feeling amongst respondents that CP97 adopted a rather prescriptive approach to the regulation of outsourcing. Several respondents pointed out that the use of outsourcing could reduce risk – where the service provider has a comparative advantage in bearing and managing certain risks. It was also felt that the costs of compliance with our outsourcing policy in CP97 would be high and the benefits relatively small, though respondents did not provide us with any data on likely costs. A request was made that we should consider the introduction of materiality thresholds, below which some of our requirements would not apply.

4.18 Issues raised were that:

- some of our requirements for the addition of particular conditions into outsourcing contracts would be difficult or expensive to achieve, or both (one key area of concern was our rule that related to audit access, see PROR 2.5.2R); and

- our policy might have a disproportionate effect on small firms, as requirements were too detailed to be sufficiently responsive to the small amount of risk posed.
**Our response:** We agree that in certain circumstances, where a service provider has a comparative advantage over a firm, outsourcing could reduce risk. However, an outsourcing arrangement carries with it particular risks that should be managed by the firm. **SYSC 3.2.4G** already guides a firm that it should have adequate arrangements ‘to supervise the discharge of outsourced functions’, and reminds it that it ‘cannot contract out of its regulatory obligations’.

Our revised *Handbook* text on outsourcing has been framed as guidance on the high level rules in **SYSC**, that a firm must establish and maintain adequate and appropriate systems and controls to manage its business prudently, and to discharge its regulatory obligations (see **SYSC 3.1.1R** and **SYSC 3.2.6R**). So, some of the outsourcing rules that were present in CP97 have now been framed as guidance. This is intended to allow firms more flexibility in determining what is appropriate to their business, in the light of the risks that they pose to our regulatory objectives.

Nevertheless, we will expect firms to adopt a suitably rigorous approach to the management of outsourcing risk. In line with our risk based approach to supervision we will also dedicate resources to reviewing the arrangements of those firms that pose the greatest risk to our objectives.
5 Compatibility with our Objectives and General Duties under the Financial Services and Markets Act 2000

5.1 This chapter explains why we believe that the proposed guidance in this CP is compatible with our general duties under section 2 of the Financial Services and Markets Act 2000 and why this is the most appropriate way to meet our regulatory objectives. The requirement for this compatibility statement is in section 155(2)(c) of the Act. The purpose of our guidance on operational risk management systems and controls is explained in Chapter 2 of this paper.

Compatibility with our statutory objectives

5.2 The operational risk management systems and controls guidance in this CP is primarily aimed at furthering three of our statutory objectives. These are, maintaining confidence in the financial system, consumer protection, and reducing financial crime. We also discuss our other objective, public awareness.

Market confidence

5.3 Confidence in the financial system is more likely to be maintained if there are high standards of market conduct, and if firms are able to meet their liabilities to their customers. Our policy is aimed at promoting both these goals. Market conduct is discussed further in relation to the protection of consumers, below. Operational risk management systems and controls help to ensure that a firm continues to be able to meet its liabilities. They do this by reducing the risk that a firm may suffer losses from business disruption (resulting either from causes external to the firm such as flood, or internal to the firm) and by preventing operational failures to identify and control appropriately financial risks arising from its business.
Protection of consumers

5.4 When considering our consumer protection objective we have, in accordance with section 5(2) of the Financial Services and Markets Act 2000, had regard to:

(a) the different degrees of risk involved in different kinds of investment or other transactions – where firms are required to have stronger controls for riskier business;

(b) the different degrees of experience and expertise that different consumers may have in relation to different kinds of regulated activity – this is not addressed directly by our operational risk policy, although, differentiation is made in our conduct of business rules and firms are required to have adequate systems to allow them to observe these;

(c) the needs that consumers may have for advice and accurate information – see below; and

(d) the general principle that consumers should take responsibility for their decisions – see below.

5.5 Operational risk is not a concept that many consumers are familiar with. Moreover, even when they are aware of operational risk they often lack the tools necessary to conduct a proper investigation into the appropriateness of a firm’s systems and controls for its management of this risk. This makes it very difficult for consumers to take full responsibility for any decisions that they make that could be affected by a firm’s exposure to operational risk.

5.6 With these issues in mind, we believe that our policy on operational risk management systems and controls promotes the achievement of this objective by giving firms additional guidance on how to meet our systems and controls requirements for risk management. In particular, this guidance is designed to support our rules in SYSC, and those proposed in PRAG 6 of CP97, which require that firms must have adequate systems and controls:

(a) to meet their liabilities when they are due;

(b) to meet the Conduct of Business standards applicable to their business;

(c) to satisfy their Client Money obligations; and

(d) that are appropriate to the business that they conduct.

5.7 In particular, we give guidance on operational risk management to reduce the risk of an operational failure in a firm’s systems and controls or a business disruption that may cause:

- it to be unable to meet its liabilities;
- the mishandling of client assets or money; and
- it to give inappropriate advice or selling to customers.
Reduction of financial crime

5.8 We have a duty, under section 6(1) of the Financial Services and Markets Act 2000, to reduce the extent to which it is possible for a business carried on by a regulated person, or in contravention of the general prohibition, to be used for a purpose connected with financial crime. Section 6(2) of the Act goes onto state that this duty requires us to have regard to the desirability of:

(a) regulated persons being aware of the risk of their business being used in connection with the commission of financial crime;

(b) regulated persons taking appropriate measures to prevent financial crime, facilitate its detection and monitor its incidence; and

(c) regulated persons devoting adequate resources to the matters mentioned in paragraph (2).

5.9 Financial crimes such as fraud or rogue trading are often opportunistic, so firms are mainly susceptible to them when their systems and controls are operationally inadequate or subject to operational failure. In the same way, a firm is mainly susceptible to money laundering where its ‘know your customer’ processes and controls are inadequate, or are poorly executed. Our guidance helps in increasing awareness of these issues by drawing a firm’s attention to how inadequate systems and controls can lead to the risk of financial crime. In addition, our guidance on operational risk management will help to reduce the amount of financial crime by encouraging firms to have systems and controls that are better able to prevent it.

5.10 Our policy also helps in the prevention of financial crime by offering guidance on certain specific topics such as: segregation of duties, so that the same employees are not involved in transaction creation and settlement; information security; and business change and continuity planning. Finally, our Handbook text in SYSC already addresses our financial crime objective by giving guidance on audit committees and internal audit functions. A firm’s audit committee and internal audit function may be useful means of assuring the effectiveness and proper implementation of its business systems and controls.

Public awareness

5.11 Our operational risk guidance is not aimed explicitly at promoting public awareness. However, it may help to stimulate public interest by highlighting a number of the major issues that firms should be considering when managing operational risk. Our guidance makes it transparent that operational risk management, and the systems and controls that a firm has for that purpose, are factors that we take into account when assessing a firm’s compliance with our general rules requiring a firm to have adequate systems and controls. As a result, knowledgeable customers may be more likely to complain about poorly performing firms that have operationally inadequate systems and controls.
Compatibility with the need to have regard to the principles of good regulation

5.12 Under section 2(3) of the Financial Services and Market Act 2000, we must have regard, in carrying out our general functions, to the following specific matters:

The need to use our resources in the most efficient and economic way

5.13 Our rules (in SYSC) already require firms to take reasonable care to establish and maintain ‘such systems and controls as are appropriate to its business’; and ‘effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime.’ Our draft Handbook text in this CP gives guidance on how firms may manage operational risk in accordance with these requirements. It has been drafted in a high level issue based manner, and as such prompts firms to consider and implement what is appropriate for their particular business and operating environment.

5.14 In addition, the PSB rules that we consulted on in CP97 require a firm to formulate and document a business plan and (operational) risk policy. This approach puts primary responsibility for the prudent management of risk on a firm, and allows us to have a dialogue with the firm about how it is managing risk in practice, rather than checking compliance with detailed requirements that may be inappropriate. Taking a high level guidance based approach also means that our policy remains appropriate as risk management practices develop.

The responsibilities of those who manage the affairs of authorised persons

5.15 As outlined above, our policy has been framed as guidance on the application of the high level systems and controls rules that are in SYSC and those that were proposed in PRAG 6 of CP97. It prompts those who manage firms to consider whether particular issues pose risks to their firms and customers, in the context of the business that they conduct, and to consider how those risks might be managed. As such, it places primary responsibility for making appropriate and effective arrangements for operational risk management with the senior managers of a firm.

The principle that a burden or restriction should be proportionate to the benefits, considered in general terms, which are expected to result from the imposition of that burden or restriction

5.16 As explained in Chapter 2 of this paper, we have an obligation under section 155 (2)(a) of the Act to publish a cost benefit analysis (CBA) when proposing new general guidance that could give rise to significant costs. A CBA is an estimate of the costs and an analysis of the benefits that may be expected to flow from the measures. We have assessed the guidance on which we are now
consulting and identified those aspects where we consider that some or all regulated firms may be exposed to significant new and additional costs. We think that the CBA in Chapter 6 of this CP shows that the costs of our proposed guidance are proportional to the benefits.

5.17 Respondents are invited to identify any areas where they think we have not identified a new additional and significant cost and to send us quantitative information to enable us to consider our CBA. Please see Question 12.

The desirability of facilitating innovation in connection with regulated activities

5.18 In developing our policy on operational risk systems and controls we have taken into account the impact that our policy may have on innovation in the market. Overall, we believe that our policy may help to facilitate innovation by raising the profile of operational risk management through bringing it to the attention of firms and their senior managers. In addition, as outlined above, we have framed our Handbook text on operational risk as guidance on our high level requirements for firms to have adequate and appropriate systems and controls, as in SYSC and PRAG 6. We do not set out detailed rules or guidance, but prompt firms to consider whether specific issues may affect their particular business, and then to make appropriate arrangements to manage the operational risks arising. This, we believe, is a flexible approach, allowing a firm’s arrangements to change in response to changes in its business, and to developments in risk management techniques. In particular, we are aware that many different computer packages are being developed to help firms identify, assess, monitor and control their operational risks in anticipation of both our own policy and international developments. We hope that our policy will stimulate further the development of such software and that firms will also find other ways to improve the measurement of operational risk, and through that its management.

The international character of financial services and markets and the desirability of maintaining the competitive position of the UK

5.19 As we explained in CP97, the PSB has generally been written to implement standards at the minimum level set out in the EC Directives, except where we consider that we need to do more to meet our statutory objectives. The EC Directives do not currently set requirements for operational risk management systems and controls. However, this topic is currently under negotiation, as outlined in Chapter 2 of this CP, and Basel and EC standards are expected in due course.

5.20 We consider that the prudent management of operational risk by firms is necessary for the achievement of our statutory objectives. We have discussed, elsewhere in this CP, that our guidance has been drafted flexibly, to permit firms to make arrangements that are appropriate to their businesses, and
proportionate to the operational risks that they face. As a result, we do not believe that our guidance will place an undue burden on firms, or adversely affect the competitive position of the UK. Better management of operational risk may, indeed, give UK firms a competitive advantage, by reducing operational losses.

The need to minimise the adverse effects on competition that may arise from anything done in the discharge of our functions

5.21 We discuss the competition effects of our policy on operational risk systems and controls in the next chapter (Chapter 6) which deals with its associated costs and benefits. Although we accept that there are costs associated with managing operational risk, we do not believe that these costs will have a significant adverse effect on competition. While firms are required to make arrangements that are adequate to address the risks that they pose to our statutory objectives, we have drafted our Handbook text as guidance. This allows firms flexibility to make the necessary arrangements in a cost-effective way.

The desirability of facilitating competition between those who are subject to any form of our regulation

5.22 We believe that our guidance on operational risk facilitates competition in the following three ways:

(a) It avoids a ‘one size fits all’ approach, which would place an undue burden on some firms.

(b) Our guidance, combined with our high level rules on systems and controls, requires that like firms, that pose like risks to our objectives, meet similar standards of operational risk management. This encourages competition between firms on the basis of the quality of service that they provide to their customers, rather than opaque and potentially risky corner cutting.

(c) Our guidance is flexible, allowing firms to determine what arrangements are appropriate for their business and we believe that our risk based approach to supervision permits us to concentrate our supervisory resources on those firms that pose the greatest threat to our statutory objectives.

The most appropriate way for us to meet our regulatory objectives

5.23 The main policy options that were open to us are assessed in the CBA in Chapter 6. To avoid being overly prescriptive, we have chosen to issue guidance on operational risk management rather than rules, and to keep this guidance at a fairly high level.
5.24 We believe that the approach in this CP is the most appropriate way to meet our statutory objectives because:

- the high level rules on risk management systems and controls in SYSC, and those that were proposed in PRAG 6, set clear requirements for firms and help to reduce risks to our objectives from operational risk management failures at firms;

- our proposed guidance sets out how our high level rules may be met in the context of operational risk management. It prompts firms to consider what issues are relevant to the business they conduct, and their operating environment, and to make appropriate arrangements to manage the risks that arise from these; and

- it places primary responsibility for the adequate and efficient management of operational risk with the management of a firm.

5.25 It is, in our opinion, the most cost-effective approach because:

- setting out clear, generally applicable policy, limits the need for repetitive explanation to different firms;

- firms can make arrangements that are proportionate to the risks that they pose to our statutory objectives;

- firms are not required to meet detailed systems and controls arrangements for regulatory purposes, that duplicate arrangements that they have for risk management purposes; and

- it is consistent with our overall risk-based approach to supervision, which seeks to ensure that while all authorised firms are subject to certain minimum standards, our resources are directed towards those firms, which pose the highest risk to our statutory objectives.

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

The aims of this cost benefit analysis

6.1 Sections 155 and 157 of the Financial Services and Markets Act 2000 require us to produce a cost benefit analysis whenever we publish draft rules or guidance, except where, under section 155(8), the costs arising from implementing the proposed rules or guidance will be of minimal significance. The purpose is to present for comment an estimate of the costs and an analysis of the benefits that will arise from the proposals being made.

6.2 We have concluded that the costs associated with implementing the draft Handbook text on operational risk systems and control that is within this CP will be of greater than minimal significance. However, we believe that many firms already have appropriate operational risk management systems and controls that are compliant with our proposed guidance. As a result, costs will be minimal for some firms, but more significant for those that decide they need to improve their operational risk management.

6.3 In what follows we set out our cost benefit analysis of the draft guidance included with this CP. We also provide a brief review of the various policy options that were open to us and explain why we believe we have chosen the most appropriate option. The main body of this cost benefit analysis distinguishes between the short-term costs of implementing this policy and the longer-term costs and benefits of complying with and supervising this policy.

Policy options

Content

6.4 The options regarding the content of our policy for operational risk systems and controls included:

- withdrawing the policy and waiting for the conclusions of the Basel and EU negotiations on operational risk;
• keeping the policy as it was in CP97;
• increasing the amount of policy and adopting a more prescriptive approach; or
• increasing the amount of policy, but adopting a less prescriptive approach, issuing guidance rather than rules.

6.5 We have chosen the last option, to increase the amount of systems and controls policy, but to frame it as guidance on the high level rules in SYSC, and those that were proposed in PRAG 6 of CP97. The benefit of this approach is that our policy is more flexible, in that it responds to the differing nature and complexity of each firm's business.

6.6 We believe that delaying introduction of the policy until the Basel 2 and CAD 3 negotiations are concluded is an undesirable option. In CP115 we stated that the chapter on operational risk systems and controls in the PSB would be published in time for the first stage of the Sourcebook’s implementation in 2004. We have already set out in our Compatibility Statement, in Chapter 5 of this CP, that the adequate management of operational risk by firms is necessary for the achievement of our statutory objectives. As a result, we believe that we should include guidance on operational risk in the Handbook, and that it should come into force in 2004.

6.7 Keeping the policy as it was presented in CP97 does not seem to be a desirable option either. Many of the respondents to CP97 requested the addition of further guidance to highlight our particular concerns about operational risk and to amplify the high level requirements for risk management that are in SYSC and PRAG 6.

6.8 Finally, we do not believe that setting detailed, prescriptive requirements for operational risk systems and controls is likely to be effective. To this end we have re-framed some of the more detailed requirements in CP97 as guidance in our revised text. The practice of operational risk management within firms can vary considerably, making it impossible to adopt a ‘one size fits all’ approach to regulation. It would also be inappropriate to expect small firms with simple businesses to adopt systems and controls that are as sophisticated as those needed by firms operating in complex environments that contain high levels of operational risk.

Location

6.9 The options regarding the location of our guidance on operational risk systems and controls included locating:
• all the policy in the PSB;
• all the policy in SYSC; or
• part of the policy in SYSC and part in the PSB.
6.10 We have chosen the last option, to locate part of the policy in SYSC and the remainder in the PSB. Three factors influenced this decision:

(a) The inadequate management of operational risk has potential adverse implications for all categories of firm, relating to their solvency, the fair treatment of their customers, and the susceptibility of such firms to financial crime. This is why there is a need for some policy on operational risk systems and controls in our high level Sourcebook for systems and controls, SYSC, where all these risks to our objectives can be addressed.

(b) In response to CP97, firms requested guidance in the PSB to help clarify our expectations on the establishment and maintenance of operational risk systems and controls in a prudential context. So, we have included some additional guidance in PRU 6.1 on the proposed PRAG 6 requirement to establish and document a business plan and (operational) risk management policy. This guidance will only apply to firms in prudential categories 1 to 4B (broadly deposit-takers, insurance firms, investment firms that take principal positions, and investment firms and Lloyd’s agents that hold client money). These are the categories of firms that represent the greatest threat to the prudential aspects of our objectives of maintaining market confidence and protecting consumers.

(c) Certain groups of firms, such as investment firms that do not take principal positions or hold client money and credit unions, are excluded from much, if not all, of our policy on systems and controls that is in the PSB. This is because we do not believe that they represent a very significant threat to our prudential objectives (see PRAG 1 in CP97). This includes a number of the general rules that relate to the establishment and maintenance of a firm’s systems and controls proposed in PRAG 6. However, we believe that the main category of risk faced by these firms is operational. So, we propose to exclude these categories of firm from the guidance on operational risk systems that will be in the PSB (consistent with credit, market, liquidity, insurance and group risk). However, these firms should consider operational risk in the context of the risks that they pose to our statutory objectives. So we have included guidance that applies to them in SYSC 3A. SYSC 1 outlines the precise scope of application for SYSC 3A, but broadly it is applicable to all regulated firms (see Annex B).
Direct costs to the FSA

Our short-term costs of implementing the new policy

6.11 Our costs are calculated on the basis of the work that we need to undertake during the 24 months that we have allowed for drafting and implementing our policy on operational risk systems and controls.

6.12 Broadly, our costs are divided into the costs of developing our policy and the costs of training relationship managers to interpret it.

6.13 The costs of developing our policy have been assessed on the basis of 1.5 full time equivalent employees working for 24 months, say 5460 employee hours. We have arrived at this figure based on the staff time that has already been devoted to this project and our estimate of the future costs that will be associated with promoting the new policy, analysing the feedback to this CP and drafting the Policy Statement. This time estimate can then be multiplied by our composite hourly charge out rate, which includes all overhead and variable costs. This rate is currently around £52 per employee hour. So, the one off cost of policy development is £283,920. To allow for contingencies, we have made this a notional charge of £280,000 to £320,000.

6.14 We estimate that many of our relationship managers will need to attend training to familiarise them with the new policy. In line with our risk-based approach to supervision this will apply particularly to those that supervise high impact Category A and B firms. Currently, we plan to organise 20 one-day training sessions, each of which will involve a maximum of 20 relationship managers. This means that a total of 2800 hours of relationship managers’ time will be spent on training. At £52 an hour the cost of this to the FSA will be £145,600. To allow for contingencies, we have made this a notional charge of £140,000 to £175,000.

Our continuing costs of authorisation and supervision

6.15 Since the policy in this CP does not require the authorisation of any new firms, no significant authorisation costs are anticipated. We may use this policy to look more closely at the practice of operational risk management, which could increase our costs of authorisation, but we do not expect this to increase significantly the cost of authorisation to firms. We have allocated a nominal cost to this of four hours per authorisation, which at £52 per hour yields a cost of £208. Assuming that in the future the number of newly authorised firms remains the same as our 2001/2002 figures of around 700 firms this will result in a cost of £145,600 per year.

6.16 We do not expect to have to recruit any new staff to monitor and enforce compliance with this policy.
Compliance costs to firms

Short term costs of implementing the new policy which will fall upon the industry

6.17 Our high level *Sourcebook* on system and controls, SYSC, already contains rules and guidance on the establishment of systems and controls that apply to a firm’s management of risk, including operational risk. In addition, we have already conducted a cost benefit analysis in CP97 for the rules and guidance that were set out in PRAG 6. The guidance that will be in SYSC 3A and PRU 6.1 is designed to support these high level rules and guidance by demonstrating how they may apply in the context of operational risk. So, for many firms there will be no new implementation costs arising from our proposed guidance. However, some firms may need to improve their systems and controls for the management of operational risk as a result of our policy.

6.18 Consultation has taken place with trade associations and other industry representatives during the drafting of this proposed *Handbook* text. These representatives were asked to comment on the likely implementation costs of our proposed policy for all sectors of the financial services industry.

6.19 Three main potential cost areas were identified:

(a) staffing costs, including senior management time, training costs and the possible recruitment of new staff to assist in implementing the policy;

(b) consultancy costs, where a firm might want to hire consultants to assist it in interpreting and implementing our policy; and

(c) IT costs, where a firm might want to buy one of the dedicated software tools that exist to help in the identification, assessment, monitoring and control of operational risk.

6.20 The size of these three cost areas could vary considerably across firms, depending on the nature, scale and complexity of their activities, and on whether they have already upgraded their operational risk management systems and controls.

6.21 In terms of IT costs, it has been suggested to us that, depending on the features of a software programme and its level of sophistication, a very large and complex firm could spend £1,000,000, or more, on installing specialised software to assist in the identification, assessment, monitoring and control of operational risk. However, most firms that decide to purchase specialist software do not, in general, spend anything like as much as this (we understand that the cost of most products range from £25,000 to £250,000). Very small firms are unlikely to need to buy any dedicated software at all. Similarly, firms will probably not need to buy any dedicated software to comply with the guidance in SYSC 3A, except perhaps for improving, where necessary, their information security. This means that those firms that are...
excluded from the guidance that will be in PRU 6.1 (such as credit unions and investment firms that do not take principle positions or hold client money) should not have to bear any significant IT costs.

6.22 In terms of staffing and consultancy costs, for prudential category 1 to 4B firms we have been informed that some larger, more complex firms have, of their own accord, already spent as much as £1,250,000 to improve their operational risk management to a standard that they consider appropriate. Our policy may cause other large and complex firms to spend a similar amount on improving their operational risk management practices, although some may decide that this is not necessary. In contrast, it has been suggested that the smaller to medium size firms in these categories that decide to upgrade their operational risk systems and controls might only invest around £25,000-£35,000 on staffing and consultancy costs. The very small could spend less. For firms that are not prudential category 1 to 4B, staffing and consultancy costs should be lower. For example, we expect that a very small category 4C or 5 investment firm that decides it needs to upgrade its operational risk systems and controls in the light of our proposed guidance in SYSC 3A might only spend a few hundred pounds. The same may apply to a very small credit union.

**Total short term implementation costs**

6.23 So, to take account of these differences we estimate that the implementation costs for category 1 to 4B firms that need to update their operational risk systems and controls will range from a minimum of £5,000 to approximately £2 million. Around 2,500 firms could incur these costs.

6.24 It is impossible at this stage to provide a reasonable estimate of the typical implementation costs for category 1 to 4B firms. This is because of the sensitivity of this cost to the size of a firm, the nature of its activities and whether it already has adequate systems and controls. In fact, we believe that a fair proportion of these firms may not need to spend anything.

6.25 The implementation costs for the remaining 6,500 or so non-category 1 to 4B firms that may need to update their operational risk systems and controls will be even lower, with compliance costs starting from around £300. Again this cost will vary quite considerably, however a fair proportion of these firms may not need to spend anything.

6.26 Since we do not plan to implement a capital requirement for operational risk at this stage, there are no additional opportunity costs associated with capital requirements.
Continuing costs of compliance which will fall on the industry

6.27 Prudential Category 1 to 4B firms may incur continuing compliance costs to meet our proposed record keeping guidance for operational risk management in PRU 6.1. However, since this guidance is designed to clarify what is already in SYSC and PRAG 6, the extent to which this will represent a separate, supplementary cost should be limited. The costs and benefits of PRAG 6 were included in the cost benefit analysis in CP97.

6.28 Firms may need to maintain their operational risk systems and controls, to ensure that they remain appropriate to their business, as well as to enhance them over time. For example, we would expect Prudential Category 1 to 4B firms to keep abreast of developments in the assessment of operational risk, as set out in the guidance in PRU 6.1. In addition, all firms will need to train new staff in their operational risk systems and controls and ensure that they review their operational risk systems and controls in the light of both expected and unexpected changes to their operations. The continuing costs of compliance with our policy will vary considerably from firm to firm and so are difficult to determine precisely. Based on our knowledge of firms we have estimated that the continuing compliance activities of firms will represent a yearly cost of around 10-20% of its initial implementation costs. This yields a cost range of around £30-£600,000 per year.

Possible future implementation costs for us and the industry

6.29 In considering the costs of our prudential policy in PRU 6.1, no attempt has been made to anticipate or allocate any of the costs that could arise out of implementation of the revised Basel Capital Accord or the EU Capital Review. This is because these costs are impossible to predict with any degree of accuracy at this time. However, firms that comply with the operational risk policy in this CP should be well prepared for the systems and controls elements of these regimes.

The short and long term benefits of operational risk regulation

Benefits to consumers and markets

6.30 As stated in Chapter 2, operational failures can cause direct losses to consumers and can have a major impact on the solvency of a firm. We believe that our proposed operational risk policy in PRU 6.1 and SYSC 3A will help to protect consumers and markets by:

- reducing a firm’s losses arising from business disruption resulting from expected or unexpected business change;
• reducing the mishandling of clients’ assets and inappropriate advice or selling to customers resulting from operational failures at a firm;

• reducing operational failure of a firm to identify, measure, monitor and control financial risks; and

• reducing a firm’s susceptibility to financial crime.

6.31 Operational risk can threaten the solvency of a firm, in particular if it is subject to a major business disruption that prevents it from paying its liabilities as they fall due. However, a firm can also suffer losses from operational failure of its general systems and controls that occurs in the ordinary course of its business, for example from system failure resulting in transaction settlement failure.

6.32 Operational risk can affect the quality of a firm’s services. Thus even where an operational risk does not affect the solvency of a firm, consumers may still lose out. For example, a consumer’s welfare may be affected by processing errors and delays (say in the payment of a particular insurance claim or the clearing of a client money deposit) or by being sold an inappropriate investment product.

6.33 Finally we believe that the draft policy in SYSC 3A will help to prevent financial crime. Many financial crimes such as fraud or money laundering can occur because firms lack adequate systems and controls for the management of operational risk.

6.34 This policy helps to reduce operational risk by:

• directing firms’ attention to the importance of operational risk management;

• highlighting the issues that a firm should consider when identifying, assessing, monitoring and controlling their operational risks; and

• providing specific guidance on some major operational risk issues such as outsourcing and business continuity management.

Benefits to individual firms

6.35 The draft guidance in PRU 6.1 and SYSC 3A on operational risk benefits firms by helping to improve transparency as set out below. In particular, this policy gives a much clearer account of the operational risk related issues that firms should be considering when complying with our high level rules and guidance on systems and control in SYSC, and those proposed in PRAG 6. This is beneficial in that firms understand better:

• how our high level standards will be applied to them; and

• how our high level standards are applied to their peers.
6.36 We also believe that firms will benefit from our decision to use guidance, rather than detailed prescriptive requirements. By having a combination of high level rules and guidance our policy is more flexible. This allows a firm to design operational risk systems and controls that fit with its general risk management systems and processes, and that are appropriate and proportionate to the risks in its business.

**Competition effects**

6.37 We do not anticipate any significant adverse competition effects, such as the erection of entry barriers or an increase in market concentration, arising out of compliance with our proposed policy on operational risk systems and controls. Although we accept that there are costs associated with compliance to this policy, we believe that the vast majority of these would be incurred in a prudent, well-managed firm even in the absence of FSA policy. Indeed firms that devote resources to the management of their operational risks might well be able to gain a competitive advantage from this, for example, through greater customer satisfaction or improved operational efficiency. We understand that many financial firms already see expenditure on operational risk systems and controls as a potential investment that can yield significant positive returns over the long run.

6.38 The relative competitive benefits of operational risk management may not be as great for small firms, particularly those that are operating with limited margins in markets where there are very large numbers of firms. However, interpretation of our guidance should be related to the nature and complexity of a firm’s activities. So, in general, we would not expect a small firm to have complex operational risk systems and controls. Our main concern for small firms is that they have an awareness of the operational risks that they face and that, as part of their normal systems and controls activities, they take steps to control these.

**Summary of costs and benefits**

6.39 The objective of this cost benefit analysis is to develop a fair estimate of the expected costs and an analysis of the benefits that will arise as a result of the operational risk policy in this CP. We think that the main costs will be one-off, arising from implementing the new policy. In contrast, the benefits of reduced operational losses to consumers and firms (achieving our statutory objectives) as well as those of improved operational efficiency and greater transparency about our expectations for the management of operational risk, will be continuing. So, on the basis of this cost benefit analysis we believe that our policy in SYSC 3A and PRU 6.1 on operational risk systems and controls will contribute to meeting our statutory objectives in a proportionate manner.
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?
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?

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

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?

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?

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?

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

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?

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?

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?

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

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?
Please note that we have decided to remove the module abbreviations PRAG, PROR, etc. and remodel the PSB in line with the rest of the Handbook, as discussed in our feedback statement to CP97 and CP115. However, for consistency we will use these old abbreviations when referring back to the draft policy that was in CP97.

This Annex contains:

**SYSC 3A**

Consequential changes to SYSC 1

Consequential changes to SYSC 3
Chapter 3A

Operational Risk: Systems and Controls
3A: Operational Risk: Systems and Controls

3A.1 Introduction

This chapter provides guidance on how to interpret SYSC 3.1.1R and SYSC 3.2.6R (which deal with the establishment and maintenance of systems and controls) in so far as they relate to the management of operational risk. Operational risk has been described as "the risk of loss, resulting from inadequate or failed internal processes, people and systems, or from external events". Thus this chapter covers systems and controls relating to risks concerning any of the firm’s operations, whether caused by internal or external matters. However, it does not cover systems and controls as they relate to credit, market, liquidity and insurance risk. Examples of operational risk exposures that the systems and controls covered in this chapter are meant to address include internal and external fraud; failure to comply with employment law or meet workplace safety standards; damage to physical assets; business disruptions and system failures; and transaction processing failures.

3A.1.2 In the context of SYSC operational risk concerns the FSA because inadequate systems and controls leading to a firm’s failure to manage it correctly can:

1. adversely affect the solvency and business operations of the firm, threatening the regulatory objectives of market confidence and consumer protection;

2. lead to the unfair treatment of the firm’s customers or the mishandling of client assets, threatening the regulatory objectives of market confidence and consumer protection; and

3. threaten the financial crime regulatory objective by making the firm more susceptible to fraud or money laundering.

3A.1.3 This guidance on operational risk systems and controls is in SYSC because operational risk is present in all firms and can affect a firm’s solvency, the fair treatment of consumers and the incidence of financial crime. This guidance deals with the management of people, processes and systems, and external events. In particular, guidance is provided on the subjects of employee responsibilities, IT systems, internal and external documentation, information security, geographic location, expected and unexpected events; business continuity, outsourcing and the role of insurance in guarding against the consequences of operational risk.

3A.1.4 Appropriate systems and controls for the management of operational risk will vary with the scale, nature and complexity of a firm’s activities. Therefore the material in this chapter is guidance. A firm should assess the appropriateness of any particular item of guidance in the light of the scale, nature and complexity of its activities as well as its obligations as set out in Principle 3 to organise and control its affairs responsibly and effectively.
3A.2 Rules and guidance on systems and controls for operational risk that are in other parts of the Handbook

3A.2.1 Many of the rules and guidance on systems and controls in the Handbook could have implications for the management of operational risk within a firm. SYSC 3A.2 does not provide an exhaustive list of all these.

3A.2.2 Specific rules and guidance for the establishment and maintenance of operational risk systems and controls in a prudential context are set out in PRAG 6 and PRU6.1 of PRU (Integrated Prudential Sourcebook). The rules and guidance in PRAG 6 and PRU 6.1 only apply to PRU category 1, 2, 3, 4A and 4B firms, however PRU category 4C and 5 firms may also find the guidance that is contained in PRAG 6 and PRU 6.1 useful.

3A.2.3 COB (Conduct of Business sourcebook) contains rules and guidance that can relate to the management of operational risk. For example, see COB 2 (Rules which Apply to all Firms Conducting Designated Investment Business), COB 3 (Advising and Selling), COB 7 (Dealing and Managing) and COB 9 (Client Assets).

3A.2.4 A firm is reminded that under PRIN 11 and SUP 15.3.1R it will need to notify the FSA of any operational risk matter that may have a significant regulatory impact. Following from SUP 15.3.8G this requirement includes, but is not limited to, notification of:

(1) a significant failure in its systems and controls;

(2) a significant operational loss; and

(3) its intention to enter into, or significantly change, a material outsourcing arrangement.

3A.2.5 A firm may also wish to notify the FSA of

(1) any significant operational exposures that it has identified;

(2) the invocation of a business continuity plan; and

(3) any other significant change to its organisation, infrastructure or business operating environment
3A.3 Areas covered by operational risk systems and controls

3A.3.1 Operational risk is a concept that can have a different application for different firms. A firm should try to understand the types of operational risk that are relevant to its particular circumstances and the impact that these risks may have on the incidence of financial crime, the fair treatment of its customers and its own solvency. This might include, but is not limited to, consideration of the following issues:

1. the inappropriate management of a firm’s people is an important source of operational risk (people refers to the employees of a firm and all other human resources that are involved in its operations);

2. both IT and manual systems and their related processes are a source of operational risk;

3. operational losses may occur as a direct or indirect result of operational risk events;

4. operational risk events may have immediate tangible effects that can be easily quantified (eg monetary) and intangible and possibly delayed effects that cannot be easily quantified (eg reputational damage);

5. the extent to which outsourced processes, people and systems remain a source of operational risk; and

6. which external events represent sources of operational risk.

3A.3.2 In establishing and maintaining systems and controls for the management of operational risk a firm should consider the full range of operational risk events that may affect its solvency, its ability to treat its customers fairly and susceptibility to financial crime.

3A.3.3 Certain frequently used risk management terms may have varied meanings in relation to operational risk. To aid in its understanding of this chapter a firm should have regard to the following interpretations that are used here:

1. a firm’s risk culture encompasses the general awareness, attitude and behaviour of its employees to risk and the management of risk within the organisation;

2. operational exposure means the degree of operational risk faced by a firm and its clients and is usually expressed in terms of the likelihood and impact of a particular type of operational loss occurring (eg fraud, damage to physical assets, etc);

3. a firm’s operational risk profile describes the types of operational risks that are faced by a firm and its clients and its exposure to these risks;
(4) A firm may also face unexpected operational losses when it is unable to evaluate with accuracy their likelihood and impact, for example due to the low frequency of their occurrence (e.g. from natural disasters).
3A: Operational Risk: Systems and Controls

Section 3A.4: People

3A.4 People

3A.4.1 SYSC 3.2.2G, SYSC 3.2.3G and SYSC 3.2.5G set out some general guidance on reporting lines and the delegation of functions within a firm, while SYSC 3.2.13G and SYSC 3.2.14G deal with the suitability of employees and agents. This section offers some additional guidance on the management of employees in the context of operational risk.

3A.4.2 The inappropriate management of a firm’s employees (and those at third party suppliers used in the performance of outsourcing arrangements) may affect both a firm’s and its clients’ susceptibility to some types of operational losses. For example, operational losses may arise as a result of breaches of fiduciary duty by employees, internal fraud or human errors.

3A.4.3 A firm should establish and maintain appropriate systems and controls for the management of operational risk that can arise from employees. This might include, but is not limited to, consideration of:

1. its operational risk culture and any variations in risk culture and human resource management practices across its operations;

2. whether the way employees are remunerated causes an increase in operational risk that threatens the ability of a firm to meet its regulatory obligations (see SYSC 3.2.18G). This might include looking at the extent to which remuneration and performance indicators reflect its tolerance for operational risk, and the adequacy of these indicators as an accurate measure of actual performance;

3. the extent of compliance with applicable regulatory and statutory requirements that relate to the welfare and conduct of employees;

4. its arrangements for the continuity of operations in the event of employee unavailability or loss;

5. the relationship between indicators of ‘people risk’ (such as overtime, sickness, and employee turnover levels) and operational losses and exposures; and

6. the relevance of all the above to employees of a third party supplier that are involved in performing an outsourcing arrangement.

Employee responsibilities

3A.4.4 A firm should ensure that all employees are aware of their responsibility and role in operational risk management, and are suitable and capable of performing these responsibilities, through the establishment and maintenance of:
(1) following from SYSC 3.2.5G, appropriate segregation of duties and supervision of employees in the performance of their responsibilities;

(2) following from SYSC 3.2.13G and 3.2.14G, appropriate recruitment and, as necessary, subsequent review processes to consider the fitness and propriety of employees, including their honesty, integrity and reputation, competence and capability, and financial soundness;

(3) appropriate systems and procedures manuals that employees may refer to as required;

(4) training processes that enable employees to attain and maintain appropriate competence; and

(5) appropriate disciplinary and termination of employment policies and procedures that are enforced.

3A.4.5 When controlling the impact that employees may have on its susceptibility to operational losses a firm should pay particular attention to the application of SYSC 3A.4.4G to approved persons and other positions of high personal trust (for example, security administration, payment, and settlement functions). Firms are reminded of the specific rules and guidance for approved persons that are outlined in other parts of the Handbook (including APER and SUP) as well as the high level rules and guidance for the apportionment of senior manager responsibilities that are contained in SYSC 2.1 (Apportionment of Responsibilities).
3A.5 Processes and systems

3A.5.1 In the normal course of its activities a firm will make use of many different systems (both IT and manual), which will, in turn, involve a variety of processes. The design, implementation and operation of these processes and systems (and those at third party suppliers used in the performance of outsourcing arrangements) may affect its susceptibility to some types of operational losses (for example, from processing errors, system failures or external fraud).

3A.5.2 A firm should establish and maintain appropriate systems and controls for the management of operational risks that can arise from inadequacies or failures in processes and systems. This might include, but is not limited to, considerations of:

1. the importance and complexity of the processes and systems used in the end-to-end operating cycle for a firm’s products and activities (for example, whether systems are sufficiently integrated, in particular for high volume business);

2. the controls that will help a firm to prevent system and process failures or identify them to permit prompt rectification (eg pre-approval or reconciliation processes);

3. whether the design and use of a firm’s processes and systems allows it to comply adequately with regulatory and statutory requirements;

4. a firm’s arrangements for the continuity of its operations in the event that a significant process or system becomes unavailable or is destroyed; and

5. indicators of process or system risk (such as reconciliation exceptions, compensation payments, and documentation errors) and actual experience of operational losses and exposures.

IT Systems

3A.5.3 IT systems includes the computer systems and information technology infrastructure required for the automation of processes and systems, such as application software, operating system software, network infrastructure, and desktop, server, and mainframe hardware.

3A.5.4 The automation of processes and systems may reduce a firm’s susceptibility to some ‘people risks’ (for example, by reducing human errors or controlling access rights to enable the segregation of duties and information security), but will increase a firm’s dependency on the reliability of its IT systems.
3A.5.5 A firm should establish and maintain appropriate systems and controls for the management of its IT system risks. This might include, but is not limited to, consideration of:

1. a firm’s organisation and reporting structure for technology operations (including the adequacy of senior management oversight);

2. the extent to which technology requirements are addressed in the business strategy;

3. the appropriateness of the systems acquisition, development and maintenance activities (including the allocation of responsibilities between IT development and operational areas); and

4. the appropriateness of the activities supporting the operation of the IT systems (including the allocation of responsibilities between business and technology areas).

3A.5.6 Internal documentation of processes and systems may reduce a firm’s exposure to some operational risks by enhancing understanding and aiding the continuity of operations. In managing its operational risks, a firm should consider the adequacy of its internal documentation, including how it is developed, maintained, and distributed.

3A.5.7 External documentation refers to the documents that are produced by a firm and provided to clients and counterparties or other third parties. A firm may use external documentation (such as contracts, transaction statements or advertising brochures) to define or clarify the terms and conditions for its products or activities, its business strategy (for example, via a press statement), or its reputational image. The presence of inappropriate or inaccurate information in these documents can lead to significant operational exposure.

3A.5.8 A firm should consider the adequacy of the processes and systems used to review external documentation prior to issuance (such as their review by the compliance, legal and marketing department or by expert external advisors). This might include, but is not limited to, consideration of:

1. the extent of compliance with applicable regulatory and legal requirements;

2. the extent to which the documentation uses standard terms (that are widely recognised, and have been validated in the courts) or non-standard terms (whose meaning may not yet be settled or whose effectiveness may be uncertain);

3. the manner in which documentation is issued; and

4. The extent to which confirmation of acceptance is required (for example, customer signature or counterparty confirmation).
3A: Operational Risk: Systems and Controls

Section 3A.5: Processes and systems

3A.5.9

Information in a firm can exist in many forms, including physical, electronic, or known to employees but not recorded. Failures in the processing of information or the security of the systems on which it is maintained can lead to significant operational exposure, with not only financial but also regulatory, other legal and reputational implications.

3A.5.10

A firm should establish and maintain appropriate systems and controls for the management of its information security risks. This might include, but is not limited to, consideration of:

(1) confidentiality: ensuring that information is accessible only to an authorised person or system (this may require firewalls within a system, as well as entry restrictions);

(2) integrity: safeguarding the accuracy and completeness of the information and its processing;

(3) availability: ensuring that an authorised person or system has access to the information when required;

(4) authentication: ensuring that the identity of the person or system processing the information is verified; and

(5) non-repudiation and accountability: ensuring that the person or system that processed the information cannot deny their action.

3A.5.11

A firm should consider the adequacy of the systems and controls used to protect the processing and security of its information and may wish to have regard to established security standards such as ISO17799 (Information Security Management).

Geographic Location

3A.5.12

The operation of processes and systems at separate geographic locations may alter a firm’s operational risk profile (for example, by allowing alternative sites for the continuity of operations). A firm should understand the effect of any differences in processes and systems at the different geographic locations.

3A.5.13

In particular, where processes and systems are operated in more than one country, a firm should consider the following non-exhaustive list of issues:

(1) the business operating environment of each country (for example, the likelihood and impact of political disruptions or cultural differences on the provision of services);

(2) the provisions of the UK Data Protection Act 1998 and EC law restrictions on the transfer of data across borders (in particular outside the EEA);

(3) the extent to which local legal and regulatory requirements may restrict a firm’s ability to meet its regulatory obligations in the UK (for example, confidentiality of customer information, and access to information by the FSA, internal audit, or external audit); and
(4) the timeliness of information flows to and from its headquarters and the compatibility with delegated authority and risk management structures.
3A.6 External events and other changes

3A.6.1

The exposure of a firm and its clients to operational risk may increase during times of significant change to its organisation, infrastructure and business operating environment. For example, a significant change may follow:

1. corporate activities such as take-overs, mergers, and demergers;
2. corporate restructuring, including the implementation, modification or termination of material outsourcing arrangements;
3. the undertaking of a new business activity or the modification of existing activities;
4. the implementation of new processes and systems or the modification of existing processes and systems;
5. invocation of a business continuity plan; and
6. changes in regulatory and legal requirements or in their interpretation by the courts.

Expected changes

3A.6.2

Before, during, and after a significant change to its organisation, infrastructure or business operating environment, a firm should assess and monitor how this change will affect its risk profile. In particular, there may be an increase in operational risk from:

1. untrained or de-motivated employees or an expected significant loss of employees during the period of change, or subsequently;
2. inadequate human resources or inexperienced employees carrying out routine business activities owing to the prioritisation of resources to the programme or project;
3. process or system instability and poor management information due to failures in integration or increased demand; and
4. inadequate or inappropriate processes following business re-engineering.

3A.6.3

A firm should establish and maintain appropriate systems and controls for the management of the risks involved in expected changes. This might include, but is not limited to, consideration of:
3A: Operational Risk: Systems and Controls

Section 3A.6: External events and other changes

(1) its organisation and reporting structure for managing the change (including the adequacy of senior management oversight);

(2) the adequacy of the programme and project management processes and systems for managing the change (including planning, approval, implementation and review processes); and

(3) communicating changes in systems and controls to its employees.

**Unexpected changes to business continuity management**

3A.6.4 High level guidance on business continuity is provided in SYSC 3.2.19G. SYSC 3A.6.4G to SYSC 3A.6.10G provides some more detailed guidance on the management of business continuity in the context of operational risk.

3A.6.5 The high level requirement outlined in SYSC 3.1.1R for appropriate systems and controls applies at all times, including following the invocation of a business continuity plan. The FSA does however recognise that there may be occasions when, because of an emergency, a firm may be unable to comply with a particular rule. The conditions for relief are outlined in GEN 1.3 (Emergency).

3A.6.6 Disruptions to the continuity of a firm’s operations can occur as a result of many different unexpected events, including loss of resources, failure of processes and systems or external events. These disruptions can result in significant operational exposures of a financial, regulatory, legal and reputational nature.

3A.6.7 A firm should consider the likelihood and impact of a disruption to its operations. This might include, but is not limited to, an assessment of:

(1) the disruptions to which it is particularly susceptible, for example:

   (a) the loss or failure of its internal and external resources (such as people, systems and other assets);

   (b) the loss or corruption of its information; and

   (c) external events (such as vandalism, war and “acts of God”);

(2) the time scale of the disruption, such as:

   (a) short term system and process failures;

   (b) medium term interruptions (such as temporary loss of resources); and

   (c) longer term disruptions (such as permanent loss of resources).

3A.6.8 A firm should implement appropriate arrangements to maintain the continuity of its operations. This might include, but is not limited to, the use of:

(1) activities to reduce the likelihood of a disruption, such as succession planning, systems resilience, dual processing and alternate service providers; and

(2) activities to reduce the impact of a disruption, such as alternate processes, contingency arrangements and insurance.
A firm should document its strategy for maintaining the continuity of its operations. This should include:

1. formal business continuity plans that outline a firm’s arrangements to reduce the impact of a short, medium or long-term disruption, including:
   a. the management framework for the implementation of the business continuity plans;
   b. the resource requirements such as people, systems and other assets, and arrangements for obtaining these resources;
   c. the recovery priorities for the firm’s operations; and
   d. communication arrangements for internal and external concerned parties (including the FSA, clients and the press);
2. escalation and invocation plans that outline the processes for implementing the business continuity plans, together with relevant contact information;
3. processes to validate the integrity of information affected by the disruption;
4. communication of the business continuity strategy;
5. processes to test the adequacy and effectiveness of its business continuity arrangements on a regular basis; and
6. processes to review and update its business continuity arrangements and plans following changes to its operations or risk profile, including changes identified from testing.

The use of an alternative site for recovery of operations is common practice in business continuity management. Where used, a firm should assess the appropriateness of the alternative site, in particular for location, speed of recovery and adequacy of resources. Where the site is shared, a firm should evaluate the likelihood and impact of multiple calls on shared resources (such as the unavailability of a third-party site due to its use by another).
3A.7 Outsourcing

3A.7.1 As explained in SYSC 3.2.4G, a firm cannot contract out its regulatory obligations and should take reasonable care to supervise the discharge of outsourced functions by its contractor. This section provides some additional guidance on the management of outsourcing arrangements, in relation to the impact that outsourcing may have on a firm’s exposure to operational risk.

3A.7.2 Firms frequently decide to outsource aspects of their operations to group companies or independent third parties, for reasons including cost, efficiency, and risk mitigation. Whilst outsourcing can bring significant benefits to firms and their clients, this may affect its exposure to operational risk through:

(1) significant changes to people, processes and systems (see SYSC 3A.6 External events and other changes); and

(2) reduced control over the people (see SYSC 3A.4 People), and processes and systems (see SYSC 3A.5 Processes & systems) used in outsourced activities.

3A.7.3 Particular care should be taken to manage material outsourcing arrangements. As explained in SUP 15.3.8G(1)(e), a firm should notify the FSA when it intends to enter into a material outsourcing arrangement.

3A.7.4 A firm’s operational risk profile will vary throughout the life cycle of an outsourcing arrangement. In managing the operational risks associated with outsourcing, a firm should consider the following non-exhaustive list of issues:

(1) its organisation and reporting structure for outsourcing arrangements (including the adequacy of senior management oversight);

(2) the extent to which outsourcing arrangements support the business strategy; and

(3) whether the firm’s contracts, service level agreements and relationship management framework allow it to monitor and control its exposure to the operational risks from the outsourcing of people, processes and systems.

3A.7.5 Before entering into, or significantly changing, an outsourcing arrangement, a firm should:

(1) analyse how the proposed outsourcing will affect its overall risk profile and business strategy and its ability to continue to meet its regulatory obligations;

(2) conduct appropriate due diligence of the service provider’s financial stability and expertise;

(3) consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement; and
(4) consider any concentration risk implications (such as the business continuity implications where a single service provider is used by several firms).

3A.7.6 In negotiating its contract with the service provider, a firm should consider the following non-exhaustive list of issues:

1. the reporting or notification requirements it may wish to impose on the service provider;

2. the extent of access available to the firm and its internal auditors, external auditors or actuaries (section 341 of the Act) and the FSA. In particular the firm should take account of its obligations under SUP 2.3.5R (Access to premises) and SUP 2.3.7R (Suppliers under material outsourcing arrangements);

3. the need for information ownership rights, confidentiality agreements and Chinese walls to protect client and other information;

4. the need for and adequacy of any guarantees and indemnities;

5. the extent to which the service provider must comply with the firm’s policies and procedures (for example, for information security);

6. the extent to which a service provider will provide business continuity for outsourced operations, and whether exclusivity agreements are needed to protect access to the service provider’s resources;

7. the management and approval process for changes to the outsourcing arrangement, including:

   a. changes in processing volumes, activities, and other contractual terms; and

   b. the ability of the firm to influence significant changes that relate to the service provider, such as a change of ownership or control, and sub-contracting;

8. the conditions under which the firm or the service provider can terminate the outsourcing arrangement, such as:

   a. a change of ownership or control (including insolvency or receivership) at the service provider or firm;

   b. significant changes in the business operations (including sub-contracting) at the service provider or firm; and

   c. inadequate provision of services that may lead to the firm’s inability to meet its regulatory obligations; and

9. the termination arrangements, including:

   a. intellectual property and information ownership rights (including any requirements for the service provider to retain or return relevant work or records); and

   b. clarifying the processes that will be followed to ensure the smooth transfer of outsourced activities to either a new third party provider or back to the firm.
3A.7.7 | In implementing a relationship management framework, and drafting the service level agreement with the service provider, a firm should consider the following non-exhaustive list of issues:

(1) the identification of qualitative and quantitative performance targets to assess the adequacy of service provision;

(2) the evaluation of performance through service delivery reports, periodic self certification or independent review by the firm’s or its service provider’s internal or external auditors; and

(3) remedial action and escalation processes for dealing with inadequate performance.

3A.7.8 | A firm should ensure that it has appropriate contingency arrangements to allow business continuity in the event of a significant loss of services from the service provider. Particular issues to consider include, but are not restricted to:

(1) a significant loss of resources at the service provider;

(2) financial failure of the service provider; and

(3) unexpected termination of the outsourcing arrangement.
3A.8 Insurance

Firms frequently take out insurance with the aim of reducing the monetary impact of operational losses. Whilst insurance can help protect a firm’s financial resources, it should consider:

1. the time taken for the insurer to pay claims (including the time that could be taken in disputing the eligibility of claims) and its funding of operating capital requirements whilst awaiting the payment of claims;

2. the financial strength of the insurer which may determine its ability to pay claims, particularly where large or numerous small claims are made at the same time; and

3. the effect of any limiting conditions and exclusion clauses, that may restrict cover to a small number of specific operational losses and may exclude larger or hard to quantify indirect losses (such as lost business or reputational costs).
Chapter 1

Application and purpose
1: Application and purpose

1.1 Application of SYSC 2, SYSC 3 and SYSC 3A

Purpose of this section

1.1.1 This section sets out the application of SYSC 2 (Senior management arrangements), SYSC 3 (Systems and controls), and SYSC 3A (Operational risk systems and controls).

1.1.2 The application of SYSC 4 (Guidance on Public Interest Disclosure Act: Whistleblowing) is set out in SYSC 4.1.1G (Application).

Who?

1.1.3 SYSC 2, SYSC 3 and SYSC 3A apply to every firm except that:

1. for an incoming EEA firm or an incoming Treaty firm:

   (a) SYSC 2.1.1 R and SYSC 2.1.2 G do not apply;

   (b) SYSC 2.1.3 R to SYSC 2.2.3 G apply, but only in relation to allocation of the function in SYSC 2.1.3 R (2) and only in so far as responsibility for the matter in question is not reserved by a European Community instrument to the firm’s Home State regulator; and

   (c) SYSC 3 and SYSC 3A apply, but only in so far as responsibility for the matter in question is not reserved by a European Community instrument to the firm’s Home State regulator;

2. for an incoming EEA firm which has permission only for cross border services and which does not carry on regulated activities in the United Kingdom, SYSC 2, SYSC 3 and SYSC 3A do not apply;

3. SYSC 2 does not apply to a sole trader as long as he does not employ any person who is required to be approved under section 59 of the Act (Approval for particular arrangements); and

4. for a UCITS qualifier:

   (a) SYSC 2.1.1 R and SYSC 2.1.2 G do not apply;
1: Application and purpose

(b) SYSC 2.1.3 R to SYSC 2.2.3 G apply, but only in relation to allocation of the function in SYSC 2.1.3 R (2) and only with respect to the activities in SYSC 1.1.4 R;

(c) SYSC 3 and SYSC 3A apply, but only with respect to the activities in SYSC 1.1.4 R.

1.1.4

(1) Question 12 in SYSC 2.1.6 G and SYSC App 1 contain guidance on SYSC 1.1.1R (1)(b) and (c).

(2) SYSC 1.1.7 R and SYSC 1.1.10 R (Where?) further restrict the territorial application of SYSC 2, SYSC 3 and SYSC 3A for an incoming EEA firm, incoming Treaty firm or UCITS qualifier.

(3) SYSC 1.1.1R (4) puts incoming EEA firm on an equal footing with unauthorised overseas persons who utilise the overseas persons exclusions in article 72 of the Regulated Activities Order.

What?

1.1.5

SYSC 2 and SYSC 3 and SYSC 3A apply with respect to the carrying on of:

(1) Regulated activities;

(2) Activities that constitute dealing in investments as principal, disregarding the exclusion in article 15 of the Regulated Activities Order (Absence of holding out etc); and

(3) Ancillary activities in relation to designated investment business.

1.1.6

SYSC 2, SYSC 3 and SYSC 3A also apply with respect to the communication and approval of financial promotions which:

(1) if communicated by an unauthorised person without approval would contravene section 21(1) of the Act (Restrictions on financial promotion); and

(2) may be communicated by a firm without contravening section 238(1) of the Act (Restrictions on promotion of collective investment schemes).

1.1.7

SYSC 3 and SYSC 3A also:

(1) apply with respect to the carrying on of unregulated activities in a prudential context; and

(2) take into account any activity of other members of a group of which the firm is a member.

1.1.8

SYSC 1.1.5 R (2) does not mean that inadequacy of a group member’s systems and controls will automatically lead to a firm contravening, for example, SYSC 3.1.1 R.
Rather, the potential impact of a group member’s activities, including its systems and controls, and any systems and controls that operate on a group basis, will be relevant in determining the appropriateness of the firm’s own systems and controls.

Where?

1.1.9  SYSC 2, SYSC 3 and SYSC 3A apply with respect to activities carried on from an establishment maintained by the firm (or its appointed representative) in the United Kingdom unless another applicable rule which is relevant to the activity has a wider territorial scope, in which case SYSC 2, SYSC 3 and SYSC 3A apply with that wider scope in relation to the activity described in that rule.

1.1.10 An example of the type of rule referred to in SYSC 1.1.7 R with a different territorial scope is the rules in COB 9.1(Custody). COB 9.1 applies, for certain UK firms, to activities carried on from branches in other EEA States as well as UK establishments. COB 1.4.3 R (c) (General application – where?). Therefore SYSC 2, SYSC 3 and SYSC 3A apply to the custody activities described in COB 9.1 carried on from such a branch by such a UK firm. The UK firm must, for example, take reasonable care to establish systems and controls under SYSC 3.1.1 R as are appropriate to those activities carried on from its EEA branches as well as from its UK establishments.

1.1.11 SYSC 2, SYSC 3 and SYSC 3A also apply in a prudential context to a UK domestic firm with respect to activities wherever they are carried on.

1.1.12 SYSC 3 and SYSC 3A also apply in a prudential context to an overseas firm (other than an incoming EEA firm, incoming Treaty firm or UCITS qualifier) with respect to activities wherever they are carried on.

1.1.13 (1) In considering whether to take regulatory action under SYSC in relation to activities carried on outside the United Kingdom, the FSA will take into account the standards expected in the market in which the firm is operating.

(2) Most of the rules in SYSC 3 are linked to other requirements and standards under the regulatory system which have their own territorial limitations so that those SYSC rules are similarly limited in scope.

Actions for damages

1.1.14 A contravention of the rules in SYSC 2 and SYSC 3 does not give rise to a right of action by a private person under section 150 of the Act (and each of those rules is specified under section 150(2) of the Act as a provision giving rise to no such right of action).
1.2 Purpose

1.2.1 The purposes of SYSC 2, SYSC 3 and SYSC 3A are:

(1) to encourage firms’ directors and senior managers to take appropriate practical responsibility for their firms’ arrangements on matters likely to be of interest to the FSA because they impinge on the FSA’s functions under the Act;

(2) to increase certainty by amplifying Principle 3, under which a firm must “take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems”; and

(3) to encourage firms to vest responsibility for effective and responsible organisation in specific directors and senior managers.

1.2.2 The main matters, referred to in SYSC 1.2.1 G (1), which are likely to be of interest to the FSA are those which relate to confidence in the financial system; to the fair treatment of firms’ customers; to the protection of consumers; and to the use of the financial system in connection with financial crime. The FSA is not primarily concerned with risks which threaten only the owners of a financial business except in so far as these risks may have an impact on those matters.
Consequential changes to SYSC 3

Insert after 3.2.5 G

G The use of inadequate systems and controls for the organisation of a firm's activities could lead to the creation of operational risk. Additional guidance on the management of employees and outsourcing arrangements in the context of operational risk is provided in SYSC 3A.4 (People) and 3A.7 (Outsourcing) respectively.

Insert as 3.2.14 (5)

G Additional guidance on the management of employees in the context of operational risk is provided in SYSC 3A.4 (People).

Addition to 3.2.18 G

G It is possible that firms' remuneration policies will from time to time lead to tensions between the ability of the firm to meet the requirements and standards under the regulatory system and the personal advantage of those who act for it. Where tensions exist, these should be appropriately managed. See also SYSC 3A.4.3G(2), which refers to remuneration in the context of operational risk.

Addition to 3.2.19 G

G A firm should have in place appropriate arrangements, having regard to the nature, scale and complexity of its business, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption. These arrangements should be regularly updated and tested to ensure their effectiveness. Additional guidance on the management of business continuity is provided in SYSC 3A.6.4G-3A.6.10G.
Please note that we have decided to remove the module abbreviations PRAG, PROR, etc. and remodel the PSB in line with the rest of the Handbook, as discussed in our feedback statement to CP97 and CP115. However, for consistency we will use these old abbreviations when referring back to the draft policy that was in CP97.
6.1 Operational Risk: Prudential Systems and Controls

Application

6.1.1 This chapter applies to a firm in PRU categories 1, 2, 3, 4A and 4B.

6.1.2 This chapter does not apply to firms in PRU categories 4C and 5; but all firms are subject to SYSC (Senior Management Arrangements, Systems and Controls) which includes high level guidance relating to operational risk.

Purpose

6.1.3 This chapter provides guidance on how to interpret PRAG 6.8.1R and PRAG 6.3.3R(2) (which relate to the design and documentation of risk management systems) in so far as they relate to the management of operational risk in a prudential context. Operational risk has been described as “the risk of loss, resulting from inadequate or failed internal processes, people and systems, or from external events”. Thus this chapter covers systems and controls relating to risks concerning any of the firm’s operations, whether caused by internal or external matters. However, it does not cover systems and controls as they relate to credit, market, liquidity and insurance risk. Examples of operational risk exposures that the systems and controls covered in this chapter are meant to address include internal and external fraud; failure to comply with employment law or meet workplace safety standards; damage to physical assets; business disruptions and system failures; and transaction processing failures.

6.1.4 Operational risk concerns the FSA in a prudential context because inappropriate systems and controls for the management of operational risk can adversely effect the solvency or business continuity of a firm, threatening the regulatory objectives of market confidence and consumer protection.

6.1.5 This chapter contains guidance on how a firm should determine, in a prudential context, its policy for operational risk management and its processes for the identification, assessment, monitoring and control of operational risk. In addition, guidance is provided on record keeping in relation to operational risk.

6.1.6 The guidance contained within this chapter is not designed to be exhaustive. When establishing and maintaining its systems and controls for operational risk a firm should have regard to other parts of the Handbook as well as the material that is issued by other industry or regulatory bodies. In particular, a firm should read this chapter in conjunction with SYSC 3A (Operational Risk Systems and Controls) which contains high level guidance on the management of people, processes and
systems, and external events in relation to operational risk. SYSC 3A also outlines some guidance on the areas that are covered by operational risk systems and controls (including the FSA’s interpretation of some frequently used risk management terms in relation to operational risk), business continuity management, outsourcing, and the role of insurance in financing operational risk. In addition, a firm should read PRAG 6, which contains the FSA’s general policy on prudential systems and controls. PRAG 6 contains some rules and guidance on which this chapter offers additional guidance.

6.1.7 Guidance on the application of this chapter to a firm that is a member of a group is provided in PRGR 2 (Group Risk Systems and Controls).

6.1.8 Appropriate systems and controls for the management of operational risk will vary with the scale, nature and complexity of a firm’s activities. Therefore the material in this chapter is guidance. A firm should assess the appropriateness of any particular item of guidance in the light of the scale, nature and complexity of its activities as well as its obligations as set out in Principle 3 to organise and control its affairs responsibly and effectively.

**General Requirements**

6.1.9 High level rules and guidance for prudential systems and controls including those for operational risk are set out in PRAG 6. In particular:

(1) PRAG 6.8.1R requires a firm in PRU categories 1, 2, 3, 4A and 4B to take reasonable steps to ensure that the risk management systems put in place to identify, assess, monitor and control operational risk are adequate for that purpose; and

(2) PRAG 6.3.3R(2) requires a firm in PRU categories 1, 2, 3, 4A and 4B to document its policy for operational risk, including its risk appetite and how it identifies, assesses, monitors and controls that risk.

**Operational risk policy**

6.1.10 Much of the management of operational risk is about identifying, assessing, monitoring and controlling failures or inadequacies in a firm’s systems and controls. As such a firm may often find that there is no clear boundary between its risk management systems for operational risk and all its other systems and controls. When drafting its operational risk policy a firm should try to distinguish between its systems and controls for credit, market, liquidity and insurance risk and its systems and controls for operational risk. Where such a distinction is not possible a firm should still try to identify those systems and controls that are used in the management of operational risk, even when they have other purposes as well.

6.1.11 A firm should document its policy for managing operational risk. This policy should outline a firm’s strategy and objectives for operational risk management and the processes that it intends to adopt to achieve these objectives. In complying with PRAG 6.3.3 R(2) the documented operational risk policy of a firm should include:

(1) an analysis of the firm’s operational risk profile (see the FSA’s interpretation of this term in SYSC 3A.3.3G(3)), including where relevant some consideration of the effects that operational risk may have on the firm and its clients;
(2) the operational risks that the firm is prepared to accept and those that it is not prepared to accept, including where relevant some consideration of its appetite or tolerance (see PRU 6.1.13) for specific operational risks;

(3) how the firm intends to identify, assess, monitor, and control its operational risks, including an overview of the people, processes and systems that are used; and

(4) where assessments of the firm’s risk exposures are used for internal capital allocation purposes, a description of how operational risk is incorporated into this methodology.

6.1.12 A firm may also wish to set threshold levels in its operational risk policy for particular types of operational risk (based on its risk appetite or tolerance for risk), which when exceeded trigger a response (such as the allocation of more resources to control the risk or a reappraisal of business plans).

6.1.13 Given its association with a willingness to take risk a firm may wish to replace the term appetite for tolerance when drafting its operational risk policy. Tolerance describes the types and degree of operational risk that a firm is prepared to incur (based on factors such as the adequacy of its resources and the nature of its operating environment). Tolerance may be described in terms of the maximum budgeted (i.e. expected) costs of an operational risk that a firm is prepared to bear, or by reference to risk indicators such as the cost or number of system failures, available spare capacity and the number of failed trades.

6.1.14 The term risk assessment can be used to represent both the qualitative and quantitative evaluation or measurement of operational exposures.

Risk identification

6.1.15 In order to understand its operational risk profile, a firm should identify the types of operational risk that it is exposed to as far as reasonably possible. This might include, but is not limited to, consideration of:

(1) the nature of a firm’s customers, products and activities, including sources of business, distribution mechanisms, and the complexity and volumes of transactions;

(2) the design, implementation, and operation of the processes and systems used in the end-to-end operating cycle for a firm’s products and activities;

(3) the risk culture and human resource management practices at a firm; and

(4) the business operating environment, including political, legal, socio-demographic, technological, and economic factors as well as the competitive environment and market structure.

6.1.16 When identifying its operational risks in a prudential context a firm should consider the full range of operational risk events that may adversely affect confidence in the financial system or the protection of its clients in relation to its ability to pay its debts as they become due.

6.1.17 A firm should recognise that it may face significant operational exposures from a product or activity that may not be material to its business strategy. A firm should consider the appropriate level of detail at which risk identification is to take place,
and may wish to manage the operational risks that it faces in risk categories that are appropriate to its organisational and legal structures.

6.1.18

The FSA’s interpretation of the term operational exposure is provided in SYSC 3A.3.3G(2).

Risk assessment

6.1.19

The FSA recognises that risk management systems for operational risk are still developing and that it may be neither feasible nor appropriate to measure certain types of operational risk in a quantitative way. A firm may wish to take a qualitative approach to the assessment of its operational risks using, for example, relative estimates (such as high, medium, low) to understand its exposure to them.

6.1.20

In order to understand the effects of its operational exposures a firm should assess its operational risks on a continuing basis. This might include, but is not limited to, consideration of:

(1) actual operational losses that have occurred within a firm, or events that could have resulted in significant operational losses, but were avoided (for example, the waiving of financial penalties by a third party as a gesture of goodwill or where by chance the firm realised profits);

(2) internal assessment of risks inherent in its operations and the effectiveness of controls implemented to reduce these risks (through activities such as self-assessment or stress and scenario testing);

(3) other risk indicators, such as customer complaints, processing volumes, employee turnover, large numbers of reconciling items, process or system failures, fragmented systems, systems subject to a high degree of manual intervention and transactions processed outside a firm’s mainstream systems;

(4) reported external (peer) operational losses and exposures; and

(5) changes in its business operating environment.

6.1.21

When assessing its operational risks a firm may be able to differentiate between expected and unexpected operational losses. A firm should consider whether it is appropriate to adopt a more quantitative approach to the assessment of its expected operational losses, for example by defining tolerance, setting thresholds, and measuring and monitoring operational losses and exposures. In contrast a firm may wish to take a more qualitative approach to assessing its unexpected losses.

6.1.22

Although a firm may currently be unable to assess certain operational risks with a high degree of accuracy or consistency, it should, according to the nature, scale and complexity of its business, consider the use of more sophisticated qualitative and quantitative techniques as they become available.

Risk Monitoring

6.1.23

In monitoring its operational risks a firm should:
(1) as appropriate, regularly report to the relevant level of management its operational exposures, loss experience (including if possible cumulative losses), and authorised deviations from the firm’s operational risk policy;

(2) engage in exception-based escalation to management of:

(a) unauthorised deviations to the firm’s operational risk policy;

(b) where set, likely or actual breaches in predefined thresholds for operational exposures and losses; and

(c) significant increases in the firm’s exposure to operational risk or alterations to its operational risk profile.

6.1.24 Risk Control

A firm should control its operational risks, as appropriate, through activities for the avoidance, transfer, prevention or reduction of the likelihood of occurrence or potential impact of an operational exposure. This might include, but is not limited to, consideration of:

(1) adjusting a firm’s risk culture and creating appropriate incentives to facilitate the implementation of its risk control strategy (see SYSC 3A.4 People);

(2) adapting internal processes and systems (see SYSC 3A.5 Processes and systems);

(3) transferring or changing the operational exposure through mechanisms such as outsourcing (see SYSC 3A.7 Outsourcing) and insurance (see SYSC 3A.8 Insurance); and

(4) providing for expected losses and maintaining adequate financial resources against unexpected losses that may be encountered in the normal course of a firm’s business activities.

6.1.25 Record Keeping

The FSA’s high level rules and guidance for record keeping are outlined in SYSC 3.2.20R (Records). Additional rules and guidance in relation to the prudential context are set out in PRAG 6.11 (Records). In complying with these rules and all associated guidance a firm should retain an appropriate record of its operational risk management activities. This may, for example, include records of:

(1) the results of risk identification, measurement, and monitoring activities;

(2) actions taken to control identified risks;

(3) where relevant, any exposure thresholds that have been set for identified operational risks;

(4) an assessment of the effectiveness of the risk control tools that are used; and

(5) actual exposures against stated risk appetite or tolerance.