INTERIM PRUDENTIAL SOURCEBOOK FOR INSURERS (SYSTEMS AND CONTROLS) INSTRUMENT 2002

Powers exercised

A. The Financial Services Authority makes this instrument in the exercise of the power in section 157(1) of the Financial Services and Markets Act 2000 (Guidance).

Commencement

B. This instrument comes into force on 1 February 2003.

Amendments to the Interim Prudential sourcebook for insurers

C. IPRU(INS) is amended in accordance with the Annex to this instrument.

Citation

D. This instrument may be cited as the Interim Prudential Sourcebook for Insurers (Systems and Controls) Instrument 2002.

By order of the Board
19 December 2002

Annex

Amendments to the Interim Prudential sourcebook for insurers

Volume Three

Guidance: FSA Guidance Notes

After Guidance Note P.2, insert the following new Guidance Note:

GUIDANCE NOTE P.3

SYSTEMS AND CONTROLS IN INSURERS

Introduction

1. The Principles for Businesses in the *FSA* Handbook set out the fundamental obligations of a *firm*. Principle 3 requires a *firm* to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

2. Senior Management Arrangements, Systems and Controls (SYSC) in the *FSA* Handbook imposes requirements to set up and maintain proper systems and controls. The rules:

   - 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*;

   - increase certainty by amplifying Principle 3; and

   - encourage *firms* to vest responsibility for effective and responsible organisation in specific *directors* and senior managers.

3. All the Principles and all aspects of SYSC apply to every regulated *firm*, not just an *insurer*. This guidance is designed to help an *insurer* comply with Principle 3 by amplifying parts of SYSC.

4. What Principle 3 and SYSC mean in practice will depend on the nature, scale and complexity of the *firm's* business. Relatively simple procedures will be enough for a one-person business, while sophisticated systems and controls are likely to be necessary for a complex organisation.

5. The term 'risk management systems' includes all levels of an organisation's management. One approach that can be taken in looking at a *firm's* overall risk management systems is to consider them in four stages:

- setting the *firm's* goals and its strategy for achieving those goals. The **governing body** (as defined in the Glossary of the *FSA* Handbook) should take responsibility for setting the *firm's* strategy and risk appetite. The points in **Annex A** of this Guidance Note about the 'Composition of the 'governing body', its role and effectiveness' will help make sure the *firm* does so;

- identifying and assessing risks. Once the *firm* has identified its strategy and assessed its business operating environment, the 'governing body' should identify and prioritise all the material risks facing the business (see 'risk assessment function' in **Annex B**);

- implementing controls. After identifying the risks, the 'governing body' should ensure arrangements are put in place to control those risks. It is obviously important that *firms* clearly document their risk and control policies (see 'Apportionment and definition of management responsibilities' in **Annex A**). 'Legal risk' - **Annex C** - and 'Outsourcing' - **Annex F** - are examples of how controls can be designed in response to particular risks; and

- monitoring and reporting how the controls are operating. 'Internal audit' (see **Annex D**) or a similar independent function should monitor controls to ensure they are appropriate and effective.

High-level controls

6. SYSC 3.2.2G says 'A *firm's* reporting lines should be clear and appropriate having regard to the nature, scale and complexity of its business. These reporting lines, together with clear management responsibilities, should be communicated as appropriate within the *firm.'*

7. SYSC 3.2.3G says:

- *'A firm's* 'governing body' is likely to delegate many functions and tasks for the purpose of carrying out its business. When functions or tasks are delegated either to *employees* or to *appointed representatives,* appropriate safeguards should be put in place.

- When there is delegation, a *firm* should assess whether the recipient is suitable to carry out the delegated function or task, taking into account the degree of responsibility involved.

- The extent and limits of any delegation should be made clear to those concerned.

- There should be arrangements to supervise delegation, and to monitor the discharge of delegates' functions or tasks.

- If cause for concern arises through supervision and monitoring or otherwise, there should be appropriate follow-up action at an appropriate level of seniority within the *firm.'*

8. **Annex A** sets out the high-level controls that an *insurer* should consider having in place. Not all of these will be appropriate to smaller *insurers*.

Risk management

9. The 'governing body' of the *insurer* will normally delegate day-to-day oversight of risk management to a risk committee. The risk committee, taking into account the risk appetite set by the 'governing body', should then consider how much risk the *insurer* is willing to take and the nature of that risk (underwriting, operational, credit, market and legal risk[1]). It should do this with reference to the overall business strategy and management expertise in each business unit. The risk committee should also establish the *insurer's* risk management policies and ensure that the risk strategy is implemented through developing and enforcing appropriate systems and controls.

Risk assessment function

10. SYSC 3.2.10G says: 'Depending on the nature, scale and complexity of its business, it may be appropriate for a *firm* to have a separate risk assessment function responsible for assessing the risks that the *firm* faces and advising the 'governing body' and senior managers on them. The organisation and responsibilities of a risk assessment function should be documented. The function should be adequately resourced and staffed by an appropriate number of competent staff who are sufficiently independent to perform their duties objectively.'

11. The manner in which the function is set up should reflect the *insurer's* own business and organisation. Where the small scale of the *insurer's* activities makes setting up a risk assessment function impractical, senior management should carry out the task.

12. *Insurers* should consider setting up a separate risk assessment function staffed by people with an appropriate mix of skills. The existence of a risk assessment function does not mean that responsibility for risk management is passed to it. Risk management should ultimately be the responsibility of the 'governing body' and those performing relevant controlled functions. In addition, line management need to be aware of their day-to-day responsibilities for managing risk in their own areas.

13. To make sure the risk assessment function is effective, *insurers* should consider putting in place some or all of the arrangements detailed in **Annex B**.

Legal risk

14. For *insurers*, legal risk is the risk that the law is proved to operate in a way adverse to the interests or objectives of the *insurer* where the *insurer*:

    - did not consider its effect;

[1] Legal risk is discussed separately in **Annex C**.

- believed its effect to be different; or

- operated with uncertainty as to its effect.

15. There are several specific systems and controls that *insurers* should consider putting in place to deal with legal risk. These are detailed in **Annex C**.

Internal audit

16. SYSC 3.2.16G gives guidance on internal audit arrangements: 'Depending on the nature, scale and complexity of its business, it may be appropriate for a *firm* to delegate much of the task of monitoring the appropriateness and effectiveness of its systems and controls to an internal audit function. An internal audit function should have clear responsibilities and reporting lines to an audit committee or appropriate senior manager, be adequately resourced and staffed by competent individuals, be independent of the day-to-day activities of the *firm* and have appropriate access to a *firm*'*s* records.'

17. Most *insurers* should have an internal audit function. In some, the function may be undertaken at *group* level for those *insurers* that are part of a larger *group,* or in exceptional cases it may be outsourced to a third party. To make sure the internal audit function is effective, *insurers* should consider putting in place the arrangements detailed in **Annex D**.

Management information

18. SYSC 3.2.11G says that: 'A *firm's* arrangements should be such as to furnish its 'governing body' with the information it needs to play its part in identifying, measuring, managing and controlling risks of regulatory concern. Three factors will be the relevance, reliability and timeliness of that information. Risks of regulatory concern are those risks which relate to the fair treatment of the *firm's customers*, to the protection of *consumers*, to confidence in the *financial system*, and to the use of that system in connection with *financial crime*. It is the responsibility of the *firm* to decide what information is required, when, and for whom, so that it can organise and control its activities and can comply with its regulatory obligations. The detail and extent of information required will depend on the nature, scale and complexity of the business.'

19. To make sure management information is effective, *insurers* should consider the detailed points in **Annex E**.

Outsourcing

20. *Insurers* often decide to outsource aspects of their operations to *group* companies, or to independent third parties. Although outsourcing can bring significant benefits to *insurers* and their customers, there is a risk that *insurers* may have reduced control of the outsourced function.

21. So, under Principle 3 of the Principles for Businesses and SYSC (3.2.3G and 3.2.4G), a *firm* should take reasonable care to supervise its outsourced functions. **Annex F**

sets out the steps a *firm* should consider taking to ensure it retains the appropriate degree of control over any outsourcing.

Group risk

22. SYSC 3 requires a *firm* to take reasonable care to set up and maintain such systems and controls as are appropriate to the nature, scale and complexity of its business. If a *firm* is a member of a *group*, it should be able to assess the potential impact of risks arising in other parts of its *group* as well as those resulting from its own activities.

23. In assessing *group* systems and controls, an *insurer* may take into account:

- its position within a *group*;
- the materiality of the *group* risk to which it is exposed; and
- the access that it has to the systems and controls of other members of its *group* and any information produced by them.

The nature and extent of the systems and controls necessary to tackle *group* risk will vary according to the materiality of those risks to the *insurer* and the position of the *insurer* within the *group*. If, for example, an *insurer* were the parent of a *group*, it would normally be responsible for ensuring that systems and controls are in place across the *group.* This would enable it to monitor and control potential risks to it because of its membership of the *group*. A small *firm* within a larger *group* should consider if there are appropriate systems and controls in place in other parts of the *group* to control such risks.

24. For *group* risk, **Annex G** sets out the systems and controls the *insurer* should consider.

Annex A (paragraph 8)

HIGH-LEVEL CONTROLS

Composition of the governing body, its role and effectiveness

A1 The 'governing body' should be composed of suitably skilled and experienced individuals who collectively have sufficient knowledge and understanding of all the *firm's* markets and products.

A2 The 'governing body' should include independent non-executive *directors* with sufficient knowledge and expertise to act as an appropriate challenge to the executive *directors*.

A3 In managing its affairs, a *firm* should have regard to such generally accepted principles of good corporate governance (including The Combined Code on Corporate Governance where appropriate) as it is reasonable to regard as applicable to it.

Apportionment and definition of management responsibilities

A4 The management structure should be clearly defined and documented and aligned with the *insurer's* business profile. There should be mechanisms in place for apportioning responsibilities in matrix management structures and for avoiding potential conflicts of interest. There should be a clear apportionment of responsibility for systems and controls in overseas branches and in all *subsidiaries*.

A5 If the *insurer* is part of a *group*, it should have the means to ensure that its statutory and regulatory responsibilities are effectively carried out, especially where the *group* is subject to matrix management.

A6 Responsibilities for the *insurer's* obligations under the Principles for Businesses (for example adequate risk management systems, handling of customer complaints, and suitability of advice) should be apportioned appropriately.

A7 The *firm* should have arrangements to make sure that approved persons in controlled functions meet the continuing requirements for fitness and propriety and have the necessary authority to perform their role effectively.

A8 There should be proper documentation of delegated authorities and means for ensuring that senior management is able to monitor delegated decisions.

A9 *Insurers* should have means for ensuring that individuals do not exceed authorities given to them to take decisions or commit the *insurer* to a transaction.

Audit committee

A10 *Insurers* should have governance arrangements that provide an element of external oversight. This function should relate to internal and external audit independently of the executive *directors* and management. *Insurer*s can achieve this in several ways, but most should consider using an audit committee (see SYSC 3.2.15G). For this committee to operate effectively, *firms* should consider putting the following arrangements in place:

- the committee should comprise an appropriate number of non-executive *directors*, one of whom should chair the committee;
- the committee should report directly to the 'governing body';
- the committee should have a formal constitution and terms of reference;
- the committee should have explicit authority to investigate matters within its terms of reference and have access to information and external advice. The terms of reference should include:
  - a role overseeing the development and implementation of a prioritised work plan for internal audit;

- ensuring that approved risk management policies and procedures are being carried out effectively and that internal controls are observed throughout the *insurer*; and

- considering reports from internal audit on issues they have identified which are of material concern;

- the committee should meet at least once a year with the external auditors in the absence of executive management.

Annex B (paragraph 13)

RISK ASSESSMENT FUNCTION

B1 The risk assessment function is a controlled function (see *SUP* 10.8.3R). The person who leads it should have sufficient expertise and influence in the *firm*. Resources should include people with an appropriate mix of skills, including underwriting, *claims* handling, accounting, actuarial and legal expertise.

B2 For some *insurers,* the risk assessment function may be integrated within their business units. In these cases the 'governing body' should satisfy itself (and monitor) that the responsibilities described below are carried out effectively.

Risk assessment function responsibilities

B3 The risk assessment function should:

- ensure that changes in the business operating environment, and in key assumptions underlying business strategies and business lines, products and business processes, and the impact of these changes on risks to the *insurer* are evaluated;

- ensure that significant new risks or material changes in significant risk (including those identified by internal audit[2] and by management information[3]) are responded to with appropriate strategies, and initiate the processes/activities to implement new risk management strategies quickly;

- ensure that the business units comply with the *insurer's* risk management frameworks through monitoring, reporting and effective communication with those responsible for risk management in the business units;

---

[2] See **Annex D**

[3] See **Annex E**

- report directly to the *insurer's* risk committee on adherence to the *insurer's* market, credit, insurance, operational and legal risk policies; and

- provide the risk committee, management and 'governing body' with meaningful risk reports and more generally ensure there is enough communication and information for the risk committee to decide on risk issues.

Annex C (paragraph 15)

LEGAL RISK

Identification and mitigation of legal risk

C1 *Insurers* should have processes for identifying which legal risks the business is exposed to, including:

- risks in existing products, including those where the interpretation of contracts could be challenged;

- the risk that a change in legislation may be overlooked or inadequately responded to;

- uncertainties surrounding existing or forthcoming court rulings; and

- risks in enforcing contracts with third parties, particularly *reinsurance* contracts.

C2 *Insurers* should also have processes for controlling (where possible) the risks that have been identified.

C3 There should be processes for reporting identified legal risks to the risk assessment function, risk committee, senior management and the 'governing body'.

C4 There should be processes for raising appropriate provisions against legal risk.

C5 Regular reviews of legal risk within the business units, including risk relating to new products, investment activities and *reinsurance*, should be undertaken.

Annex D (paragraph 17)

INTERNAL AUDIT

Mandate/terms of reference of internal audit (IA)

D1 The objectives and responsibilities of IA should be clear and an audit committee or alternative (see below) should approve the terms of reference for IA.

D2 The scope of IA's remit should be clear and appropriate for the risks run by the *insurer*, including those risks arising from proposed new lines of business or products.

D3 IA should have access to all the appropriate books and records of the *insurer* it considers are necessary to carry out its responsibilities.

D4 Any operational work undertaken by IA (such as special projects) should not compromise its independence. IA's relationship with the *insurer's* external auditors should be full, open and frank.

Reporting lines and resources

D5 IA should have an independent reporting line to the audit committee[1], where one exists. In those cases where the *insurer* does not have an audit committee, the reporting line should be to a non-executive member of the 'governing body' (preferably a non-executive chairman where there is one). IA should have unfettered and regular access to the audit committee (or the non-executive *directors*). Also, IA should have full and regular access to the chairman and CEO of the *insurer*.

D6 The Head of IA should be a senior and experienced individual who is an employee of the *insurer*, or the *group* of which the *insurer* is a part. This post is a controlled function (see *SUP* 10.8.3R).

D7 IA should have enough suitably qualified and experienced staff to complete the audit plan, including auditing those areas that require detailed technical or local knowledge. IA staff should be credible with senior management, external auditors and the audit committee. They should be able to act as an effective challenge to the business and support areas.

Audit plan

D8 The audit committee (or alternative) should approve an audit plan. The plan should include the audit of all appropriate business and control areas within the *insurer*, including the compliance function. There should be a clear, formal, risk-based process (see below) for deciding which areas to include in the plan. The plan should be reviewed at least once a year.

D9 The plan should allow for (but not be compromised by) other IA responsibilities such as special projects, fraud investigations and new product approval processes.

Methodology

D10 IA should use risk-based methodologies. There should be clear definitions and rationale for any scoring systems used to support the risk-based approach.

---

[1] for audit work. For staffing and resource issues, IA can report to another part of the *insurer*.

D11 There should be processes for alerting senior management and the audit committee (or alternative) quickly to higher risk issues uncovered by IA and for responding to incidents, including the setting up of investigations led by IA.

Audit reports and subsequent actions

D12 There should be a process for communicating, and agreeing, IA reports with the business or support areas under review. Issues raised in IA reports should be clear and prioritised for action, and the 'owner' of the action point should be identified. Reports should be timely and, where necessary, reports should be graded (for example 'green', 'yellow', 'red'). They should be distributed to the appropriate senior management.

D13 There should be processes for ensuring recommendations raised in IA reports are dealt with in a timely fashion and processes for monitoring outstanding exceptions or recommendations. These processes should include external recommendations from auditors or others. There should be an escalation process for recommendations or exceptions that line management have not dealt with.

Outsourcing internal audit

D14 An *insurer* should not normally outsource its IA either to those who produce skilled persons reports for it or its external auditors. However, there may be circumstances where certain IA services are better provided by the external auditors/skilled persons - for example, where specialist technical knowledge is needed to act as an effective challenge to a business or support area. In these cases the following conditions should be met:

- the work should be carried out under the overall supervision and management of the *insurer's* own internal audit staff; and
- ultimate responsibility for the adequacy and effectiveness of IA should lie with the Head of IA.

Annex E (paragraph 19)

MANAGEMENT INFORMATION

E1 The *insurer* should have management information (MI) which is sufficient to identify, measure and control all the material risks in the business including new products and new business.

E2 MI should be timely to enable prompt action to be taken where necessary.

E3 It should be detailed enough (without being so detailed as to lose impact) for the various levels of management (including the 'governing body') that use it.

E4 Where relevant, it should cover the activities of branches or *subsidiaries*.

E5 MI should not just be about static historical data, but also consider the possible range and variability of potential outcomes. So it should:

- include the results of stress and scenario testing (including the valuation of assets and movements in liabilities) to help the *insurer* identify the financial impact of risks in different scenarios; and

- measure the ability of the business to withstand adverse conditions over a prolonged period.

E6 Examples of other types of MI that *insurers* might produce (according to their size and spread of business) include:

- profit and loss, etc. (including technical underwriting results) for significant business/geographic areas or product lines;

- comparison to budgets and explanation of variances;

- risk/reward information, capital used and allocation;

- customer acquisition and loss;

- customer satisfaction measures and complaints;

- performance of service providers;

- market share data;

- compliance with regulatory requirements (financial and other); and

- information on all risks facing the business including underwriting, credit, market and operational risks (for example, processing and documentation errors, *claims* handling, business interruption, financial crime) and legal risk.

Annex F (paragraph 21)

OUTSOURCING

Issues to consider when entering into an outsourcing arrangement[1]

F1 Before entering into, or significantly changing, an outsourcing arrangement, an *insurer* should:

---

[1] See **Annex D** for the outsourcing of internal audit

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

- conduct appropriate due diligence of the service provider's financial stability and expertise;

- consider how it will ensure a smooth transition of its operations from its current arrangements to a new or changed outsourcing arrangement; and

- consider any concentration risk implications (such as business continuity implications where several bodies use a single service provider).

The contract with the supplier

F2 In negotiating its contract with the service provider, the *insurer* should consider:

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

- the need for information ownership rights, confidentiality agreements and appropriate segregation to protect client and other information;

- the need for and adequacy of any guarantees and indemnities;

- the extent to which the service provider must comply with the *insurer's* policies and procedures (for example, information security);

- 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;

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

  – changes in processing volumes, activities and other contractual terms; and

  – the ability of the *insurer* to influence significant changes by the service provider, such as change of ownership or control, and sub-contracting;

- the conditions under which the *insurer* or the service provider can terminate the outsourcing agreement, such as:

  – a change of ownership or control (including insolvency or receivership) at the service provider or *insurer*;

  – significant changes in the business operations (including sub-contracting) at the service provider or *insurer*; and

- inadequate provision of services that may lead to the *insurer's* inability to meet its regulatory obligations; and

- the termination arrangements, including:

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

  - 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 *insurer*.

F3 Also, the *insurer* should include a requirement that the supplier gives the *insurer's* internal and external auditors the same rights as are given to an auditor by section 341 of the *Act* (see *SUP* 2.3.9G).

Relationship management framework/service level agreement

F4 In implementing a relationship management framework, and drafting the service level agreement with the service provider, the *insurer* should consider:

- the need for an adequate flow of management information from the supplier to the *insurer*;

- the identification of qualitative and quantitative performance targets to assess the adequacy of service provision;

- the evaluation of performance through service delivery reports, periodic self-certification, and/or independent review by the *insurer's* or service provider's internal or external auditors; and

- remedial action and escalation processes for dealing with inadequate performance.

Contingency arrangements

F5 The *insurer* should make sure 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:

- a significant loss of resources at the service provider;

- financial failure of the service provider; and

- unexpected termination of the outsourcing arrangement.

GROUP RISK

Insurer's responsibilities for group systems and controls in general

G1 The *insurer* should take reasonable care to set up and maintain such systems and controls as are appropriate for:

- monitoring the effect on the *insurer* of its relationship with other members of the *group* and the activities of other members of its *group*;
- monitoring compliance with the *group* capital reporting requirements where these apply to the *insurer* and with concentration risk requirements;
- monitoring liquidity within the *group*; and
- monitoring compliance with *group* risk reporting controls.

Relationships within the group

G2 The overall governance, high-level controls and reporting lines within the *group* should be clear. The *insurer* should not be subject to material control or influence from other parts of the *group* that is exercised through informal or undocumented channels.

G3 The linkages between *group* central functions (for example, *group* risk management, capital planning, liquidity, compliance) and the *insurer* should work effectively and the *insurer's* approved persons structure should reflect the extent to which *group* functions influence it.

G4 Potential conflicts of interest, where other *group* companies undertake activities in areas related to the *insurer*, should be minimised by using, for example, chinese walls, and transactions at *market value*.

G5 The *insurer* should have procedures in place to make other *group* companies aware of the *insurer's* regulatory obligations.

G6 The *insurer* should have procedures in place to be informed of events in the *group* (including financial crime, financial weakness, customer mis-selling, failures of controls) that may have an impact on the *insurer's* ability to comply with its regulatory capital or other requirements. The *insurer* should have plans in place to minimise the effect of these events on its own business.