



Toolkit for Risk-based
pensions supervision

Module 4
Risk Mitigants
and Risk Scoring

Introductory note

Risk-based Pensions Supervision provides a structured approach focusing on identifying potential risks faced by pension funds and assessing the financial and operational factors in place to mitigate those risks. This process then allows the supervisory authority to direct its resources towards the issues and institutions which pose the greatest threat.

The **IOPS Toolkit for Risk-based Pensions Supervisors** provides a 5-module framework for pensions supervisors looking to apply a system of risk-based supervision. A web-based format allows: a flexible approach to providing updates and additions; users to download each module separately as required; and a portal offering users more detailed resources, case studies and guidance. The website is accessible at www.iopsweb.org/rbstoolkit.

This document contains the guidance for **Module 4: Risk Mitigants and Risk Scoring**

This work is published on the responsibility of the International Organisation of Pension Supervisors (IOPS). This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

IOPS freely authorises the use of this material for non-commercial purposes. Requests for commercial use or translation of this material should be submitted to daf.contact@oecd.org.

© IOPS 2012

TABLE OF CONTENTS

INTRODUCTION	4
A. Purposes	4
B. Principles and Guidelines	6
SECTION 1: RISK MITIGANTS	7
A. Risk Mitigants	7
B. Pension Funds' Risk-management Systems	13
SECTION 2: WEIGHTING RISKS- PROBABILITY AND IMPACT	20
A. Weightings.....	20
B. Probability	24
C. Impact.....	30
SECTION 3: CONSISTENCY OF SCORES.....	33
BIBLIOGRAPHY.....	38

INTRODUCTION

Risk-based supervision (RBS) is a structured approach which focuses on the identification of potential risks faced by pension plans or funds¹ and the assessment of the financial and operational factors in place to minimise and mitigate those risks. This process then allows the supervisory authority² to direct its resources towards the issues and institutions which pose the greatest threat.

A. Purposes

Having identified the major risks to meeting its supervisory objectives (see Module 3 of the IOPS Toolkit), the pension supervisory authority needs to consider possible mitigants and controls so that risk is assessed on a *net* rather than a *gross* basis. The authority then needs to establish a method for weighting these risks, according to the probability of their occurrence and their importance and impact on the goals of the supervisory authority – *i.e.* a risk scoring model has to be devised.

Some pension supervisory authorities derive individual risk-scores for the entities which they oversee. Such methods can help supervisory authorities devise an efficient, proportional, consistent and truly risk-based approach. Their purpose is to integrate qualitative and quantitative factors, to help identify areas for attention by institutions and to help establish supervisory priorities. The danger, and difficulty, with such models is to allow for sufficient individual judgement in their use, and to stop them becoming simply 'box ticking' exercises. A balance needs to be struck between designing a system which is sufficiently complex to be able to capture and assess a wide range of risks at the firm specific and generic level and which can operate across a widely varying regulated population, and yet be simple enough to be understood and used on a day to day basis by supervisors.

¹ According to the OECD's taxonomy (OECD 2005), a pension fund is a legally separated pool of assets forming an independent legal entity that is bought with the contributions to a pension plan for the exclusive purpose of financing pension plan benefits. The plan/fund members have a legal or beneficial right or some other contractual claim against the assets of the pension fund. Pension funds take the form of either a special purpose entity with legal capacity (such as a trust, foundation, or corporate entity) or a legally separated fund without legal capacity managed by a dedicated provider (pension fund management company) or other financial institution on behalf of the plan/fund members.

A pension plan is a legally binding contract having an explicit retirement objective (or – in order to satisfy tax-related conditions or contract provisions – the benefits cannot be paid at all or without a significant penalty unless the beneficiary is older than a legally defined retirement age). This contract may be part of a broader employment contract, it may be set forth in the plan rules or documents, or it may be required by law. In addition to having an explicit retirement objective, pension plans may offer additional benefits, such as disability, sickness, and survivors' benefits.

In EU countries, this module may not apply to those pension funds and pension plans that fall outside the scope of the EU Directive 2003/41/EC of the European Parliament and of the Council of 3 June 2003 on the activities and supervision of institutions for occupational retirement provision, *e.g.* pensions funded via book reserves.

² Pension supervisory authorities referred to in the IOPS Toolkit are defined as any entity responsible in whole or in part for the supervision of pension funds, plans, schemes or arrangements in a country, or the subdivision of a country, whether invested with its own personality or not.

However, it may not be feasible for supervisory authorities to derive an individualised risk score for every single supervised entity – particularly in pension systems where many thousands of funds operate. In such cases, supervised entities are categorised in a simplified way – usually in terms of their size or impact of failure– with the funds which have the greatest ‘impact’ receiving the greatest supervisory attention (as described in Module 5 of the IOPS Toolkit).³

As the individual country case studies provided in the IOPS Toolkit show, many supervisory authorities around the world have already developed their own risk-scoring models. Clearly others can learn from these, but the IOPS Working Paper No.4 (IOPS 2007) urges caution, pointing out that one of the first challenges faced by the IOPS members when beginning their move to a risk-based approach to supervision was how to adapt existing models and approaches from other countries and sectors. A simple, but fundamental lesson learnt by IOPS members is that one model or structure cannot be taken from one country and applied unaltered to another pension system. All countries are unique, with models requiring adaptation to each situation. The message from IOPS members is to look widely and decide what would be appropriate for the individual pension system before trying to adapt one model.⁴

A further lesson stressed by IOPS members in the Working Paper is that any model, once built, should not be considered as fixed in stone. For example, one of the pioneers in risk-based supervision, the Australian Prudential Regulation Authority (APRA) of Australia, point out the need for flexibility and time to adapt to the inevitable introduction related problems. Even if the system is ‘close to correct’ time is still required to let it ‘embed’. Regarding APRA’s risk scoring system (Probability and Impact Rating System known as PAIRS), they acknowledge that the staff were fairly negative for the first six months, and it took a full 18 months or so to be accepted, and a full three years from introduction for modifications to be included. APRA’s message is therefore think ‘increment and evolution’ – “get it as right as possible, give it time to embed and expect to have difficulty with this but also expect to make changes in the future.”

One structural mistake which all authorities which contributed to the report felt they made was rolling out their new system live to all funds at the same time. All agreed that running a ‘pilot’ project with a few funds - to test data collection and other administrative issues, as well as internal staff capability etc. – would have been extremely useful. APRA also suggest that an assessment should be made whether the system needs to be different for different categories/classes of funds.

This Module 4 of the IOPS Toolkit is designed to help supervisory authorities who wish to build a risk-scoring model which will be used to guide their supervisory actions. Risk mitigants are first discussed, to help supervisors consider risk on a net basis. The Module then goes on to consider how to weight the components of risk scoring models in order to devise a final score and how to check for consistency in such scores.

³ As noted in the Introduction to the IOPS Toolkit, risk-based supervision can sometimes be confused with these individual risk-scoring models – indeed it can be thought that risk-based supervision *is* simply such a risk-scoring model. However – as the IOPS Toolkit strives to show – RBS is a much broader philosophy or approach which can be implemented even when detailed analysis on each individual institution is not feasible.

⁴ Trying to adapt an ‘intra-country’ model may be just as difficult, due to differences between sectors. For example, the Pensions Regulator (TPR) in the United Kingdom started by adapting an approach from the United Kingdom’s Financial Services Authority. However, it quickly became apparent that this would not work for TPR as it would not be practical to score each of the thousands of pension plans in the United Kingdom individually.

Figure 1: Risk-based Supervision Process



Source: IOPS Secretariat

B. Principles and Guidelines

This Module 4 of the IOPS Toolkit builds on the *IOPS Principles of Private Pension Supervision*:⁵

Principle 5: Risk-based Supervision

Pension supervisory authorities should adopt a risk-based approach

5.1 In order to use their resources efficiently, pension supervisory authorities should adopt a risk-based approach, and a suitable risk-assessment methodology should be established.

5.8 Risk-scoring models should reflect the risk-focus of the pension supervisory authority (which is driven by its objectives and resources), and the net risk of relevant individual entity and systemic risk factors. These factors should be suitably weighted according to the nature of the pension system, and a risk-score derived from the probability and impact of their occurrence.

⁵ See (IOPS 2010a)

SECTION 1: RISK MITIGANTS

A. Risk Mitigants

Many risks can be effectively controlled or reduced to acceptable levels. Consequently, in addition to risk factors (which are discussed in Module 3 of the IOPS Toolkit), to have a truly risk-based approach supervisors need to look at mitigating factors which lower these risks – *i.e.* they analyse risk on a *net* rather than a *gross* basis.

Figure 2: Example of Net Risk Scoring

		Level of Inherent Risk for Significant Activity			
		Low	Moderate	Above Average	High
Quality of Risk Management for Significant Activity	Strong	Low	Low	Moderate	Above Average
	Acceptable	Low	Moderate	Above Average	High
	Needs Improvement	Moderate	Above Average	High	High
	Weak	Above Average	High	High	High

Source: Toronto Centre

Figure 3: Example of a Risk Matrix

RISK MATRIX					
Significant Activities	Materiality	Inherent Risks	Quality of Risk Management	Net Risk	Direction Of Risk
Activity 1	★	<input type="checkbox"/> Credit <input type="checkbox"/> Market <input type="checkbox"/> Liquidity <input type="checkbox"/> Insurance <input type="checkbox"/> Operational <input type="checkbox"/> Legal & Regulatory <input type="checkbox"/> Strategic	Operational Management <input type="checkbox"/> Oversight <input type="checkbox"/> Financial Analysis <input type="checkbox"/> Compliance <input type="checkbox"/> Internal Audit <input type="checkbox"/> Risk Management <input type="checkbox"/> Senior Management <input type="checkbox"/> Board Oversight	★	
Activity 2					
Etc...					
Overall Rating	Overall Assessment				

Capital	Earnings		
Composite Risk	★	Direction of Risk	Time Frame

Source: Toronto Centre

Risks can be managed in a variety of ways, including good corporate governance, a capable senior management team, well-documented procedures, strong internal controls, an independent internal audit function (or equivalent services provided by an audit firm), effective risk management processes, strong actuarial and financial analysis capabilities, and comprehensive external audits. Some risks may be managed financially, e.g. using reinsurance, hedging or securitisation.⁶

The main mitigating factors which supervisory authorities may wish to consider include the following – though it should be noted that not all factors will be relevant for all types of pension system:

- **Risk Mitigants**

- **Quality of the governing board / trustees:** covers their understanding of responsibilities, their experience, competence and integrity and the presence of conflict of interest. If there are concerns about the probity of those in control, this would increase the risk score. The degree of *trustee oversight* is also key- meaning overall plan governance, and in particular the strategic direction of the plan, as well as the relationship between the plan sponsor and the Trustees. There is a degree of subjectivity in rating this factor. Negative scores would be recorded if filings are late and/or incomplete, or if the plan does not fully cooperate with the pension supervisory authority. Lack of proper control and lack of proper documentation would also

⁶ For example, in Hong Kong, Mandatory Provident Fund (MPFA) trustees are required to take out adequate insurance to indemnify plan members against any loss of plan assets caused by misfeasance or misconduct of the trustees or their service providers. There is also a statutory Compensation Fund set up to compensate plan members should the indemnity insurance not fully cover those losses. The government has injected HK\$600m as seed money into the Compensation Fund. When in need, the MPFA may apply to the courts to make use of the fund.

increase the score. In-depth inspections would be able to deepen the analysis of this factor.

- **Management controls:** comprises management quality and structure, decision making process, strategic planning process and risk control attitude. Management should enable mitigation of inherent risk through a management structure and composition in line with the volume, scope and complexity of the business, clear and comprehensive allocation of responsibilities and adequate management oversight and control, including fostering a culture of risk and control awareness.
- **Compliance culture and procedures:** relates to compliance with laws and regulations and involves assessment of the competence, integrity and independence of responsible staff, as well as a fund's information systems
- **Effectiveness of operational management:** includes human resource policies and management of outsourced operations by the governing board. Organisational controls comprise the pension fund structure, group relationship, reporting lines and responsibility structure. Organisation enables mitigation of inherent risk by a transparent organisation structure, clear relationships between activities, management units, and group functions, adequate reporting on all levels and an adequate responsibility and authorisation structure. Capacity to produce timely and reliable information for regulators and members should also be considered. This factor includes the issue of efficiency of administration, in terms of expenses. Lack of completion of questionnaires, interrogatories, or the like, or unsatisfactory completion would add to the score. Unsatisfactory filing record, including history of late payment of contributions, would also add to the score. If there are outstanding complaints this would add a further amount to the risk score. Expenses per member that are significantly above the average would also add to the risk score. Any other negative features, including lack of cooperation during on-site inspections, would add further to the score.
- **Adequacy of risk management systems:** quality of arrangements for identifying and measuring risk, setting limits, monitoring compliance and reporting. Risk-specific controls comprises the risk management framework, financial and management reporting, operations risk controls, audit controls, compliance controls, IT controls and HR controls. Internal controls enable mitigation of inherent risk by timely and appropriate identification, measurement, monitoring and management of all risks.
- **Adequacy of independent review:** this factor refers to the independence and competence of the actuary and the auditor and the quality of their reports. Internal and external audit and actuarial reviews require assessment of both competence and independence. Reliable independent review will give the pension supervisory authority greater confidence in the administration, funding and investment of the pension plan. If the actuary is an employee of the sponsor, this would add a component to the risk score, although this is not necessarily a strong negative, if the actuary demonstrates independence. If there are any other concerns about the professionals (for example, not members in good standing in the respective national or international professional bodies), then a further risk score would be added. If reports are difficult to follow or are not well prepared or have qualifications, an additional risk score would be added.
- **Role of administrator:** e.g. where an administrator has proven track record, this might mitigate some of the risk factors identified, though analysis should focus on what controls are actually in place to decide whether they are likely to be effective in mitigating specific types of risk in future.
- **Sponsor:** i.e. the employer contributing to the fund – information may also be useful –

especially in a defined benefit (DB) environment (as an employer with a strong financial position may be considered to be a more reliable contributor to the pension plan in future).

- **Financial support:** defined benefit (DB) funds (and defined contribution (DC) funds which offer guarantees) with higher levels of financial reserves are more likely to be able to pay promised pension benefits. The level of these reserves can therefore be considered as a risk mitigant (protecting against the ultimate risk of not receiving promised or expected retirement income). The results of the types of quantitative risk assessment described in Module 2 of the IOPS Toolkit therefore feed into the overall risk assessment by way of mitigating considerations (e.g. by way of the bar showing solvency, on-going performance and funding in the Office of the Superintendent of Financial Institutions, Canada (OSFI) risk matrix below).

- **Risk Matrix: Office of the Superintendent of Financial Institutions, Canada**

Significant Activities	Inherent Risks					Quality of Risk Management		Net Risk
	Investment	Pension / Valuation	Operational	Legal and Regulatory	Strategic	Controls	Oversight	
Actuarial								
Administration								
Asset Management								
Communication to Members								
Overall Net Risk								

Solvency		Ongoing Performance		Funding	
----------	--	---------------------	--	---------	--

CRR:	
Direction:	

Source: OSFI (2009a+b)

Just as risks need to be considered on a systemic basis (as discussed in Module 3 of the IOPS Toolkit), risk can also be mitigated on a system-wide basis. For example, if longevity risk is a particular concern, this can be mitigated by including increases in life-expectancy in the assessment of pension liabilities. Where the governance of pension funds is found to be a system-wide risk, this can be mitigated by focusing on pension fund trustee or fiduciary knowledge and understanding. As system-wide risks will often be mitigated by supervisory responses and interventions, the issue is discussed in further detail in Module 5 of the IOPS Toolkit.

Not all potential risk management tools – financial or non-financial –are equally applicable or effective in managing each type of risk. Accordingly, before attempting to assess a pension fund’s management of its risks, the supervisor must not only have a clear understanding of these risks but also know which risk management tools are most relevant to each. Industry benchmarking can be useful in identifying best practices and establishing assessment criteria that the supervisory staff can use (e.g. in order to assess the contribution of internal audit, the supervisor should know the characteristics of a good internal audit function – such as its responsibilities, authority, reporting relationships, staff

capabilities and methodology). Although assessment against these criteria would seem to lend itself well to a checklist approach, the supervisor must nevertheless apply judgment during this process.⁷

Where a fund has outsourced its operations, and if the operations relate to pension business, the supervisor needs to assess the systems of the external parties as well as the protections that the pension fund has under its contracts with these parties as the governing board of the pension fund has the ultimate liability for any shortcomings out of the outsourced operation. Supervisory reviews should include the right to directly address and request information from a pension fund’s service providers - or the pension supervisory authority should have mechanisms in place for liaising with other financial service authorities in order to do so.⁸

Example: Australia



For the following risk categories the Australian Prudential Regulation Authority (APRA) produces a quality assessment score for both inherent risk and a separate quality assessment score for the management and controls relevant to that risk. The net risk position of each category is a simple average of the two quality assessment scores.

Risk Category	Principle determinant in APRA’s assessment of Management and Control
Liquidity Risk	<ul style="list-style-type: none"> • Awareness of liquidity risk by the Board • Liquidity management functions and committees (ALCO) in place • Policies and procedures relating to liquidity risk management • Limits in place and how they are reviewed and monitored • Scenario analysis and models used, including dependability of information sources • Reliability and extent of intra-group funding and standby facilities

⁷ In some areas it can be difficult to identify the difference between a risk and a control –with financial regulators in particular encountering this problem especially in periods of financial crisis. For example, some may see derivatives as control mechanisms (to hedge current or interest rate risk, for example) – where as others could view these contracts as risks in themselves. Indeed the danger that some techniques used to mitigate one type of risk can themselves create other types of risk. Therefore the interrelationships should carefully be considered. See (Black 2008) p.30.

⁸ For further details see (IOPS 2010c), ‘Managing and Supervising Risk in Defined Contribution Pension Systems’.

	<ul style="list-style-type: none"> Contingency arrangements in place, including any contributions to multilateral liquidity support arrangements
Operational Risk	<ul style="list-style-type: none"> The awareness of operational risk by the Board Operational risk management functions and committees Policies and procedures Controls in place across the IT environment Management of operational issues including administration, outsourcing arrangements, new products, project management and fraud Business continuity and disaster recovery plans, including testing processes in place and back up arrangements such as data files, documentation, regularity of file recovery and off-site location (and testing of such arrangements)
Credit Risk	<ul style="list-style-type: none"> The awareness of credit risk by the Board The credit risk management framework, systems and delegations in place Origination, security and collateral structures and valuation practices Credit-related policies and procedures Problem asset management including compliance with prudential requirements Information systems and portfolio management The role and functioning of independent credit review process
Market and Investment Risk	<ul style="list-style-type: none"> The awareness of maker an investment risk by the Board Trading and investment functions, including segregation of responsibilities ALCO and /or investment committees in place Delegations and limits in place and how they are monitored and controlled The process of reviewing and monitoring trading and /or investment strategies

- | | |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • Investment management and asset valuation practices • Market and investment policies and procedures including those relating to unit pricing • Models used, including underlying assumptions and stress analysis • The strength of management information systems • Independent review functions |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

B. Pension Funds' Risk-management Systems

Whatever the nature of the pension system being overseen, the focus of the analysis of risk mitigants should be on the pension funds' risk-management systems. As described in IOPS Working Paper No. 11 (IOPS 2009a)⁹ risk-management systems can be defined as the process - effected by an organisation's governing board, senior management and other personnel - designed to provide reasonable assurance regarding the achievement of objectives in terms of: effectiveness and efficiency of operations; reliability of financial reporting; compliance with laws and regulations.¹⁰ The process does not involve just one policy or procedure performed at a certain point of time but should be continually operating at all levels of the organisation, and involve all staff.

Risk-management systems can be broken down into four broad categories:

- *Management Oversight and Culture* - including board responsibilities, organisational structure, control culture, code of conduct;
- *Strategy and Risk Assessment* - covering areas such as risk strategy, operational risk management, investment strategy;

⁹ See also IOPS/OECD *Good Practices for Pension Funds' Risk Management Systems* (IOPS 2010b)

¹⁰ The Committee on Sponsoring Organizations of the Treadway Commission (COSO) established a common definition of internal control that services the needs of different parties for assessing and improving their control systems. http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990009/PC-990009.jsp

- *Control Systems* - IT systems, monitoring systems, internal audit and external controls;
- *Information, Reporting and Communication*.

Each financial institution's particular approach to risk management will vary with the size and nature of its business, along with the stage of development of the markets in which it operates. Risk-based supervision can be successfully implemented even in jurisdictions where the financial institutions themselves may not be employing sophisticated risk management techniques – though greater supervisory oversight and other risk control measures (such as quantitative investment rules) will still be required where this is the case. Whatever the situation, it is essential that supervisory assessments consider not only the existence of policies, procedures and controls, but also their effectiveness as risk management tools.

As explained in Module 1 of the IOPS Toolkit, the supervisory authority may wish to provide guidance to supervised entities on the risk management systems and other forms of mitigants they would expect to see. Indeed (again as discussed in Module 1 of the IOPS Toolkit), providing such guidance to overseen entities is an important element in RBS, which may be new and have to be developed by supervisory authorities adopting this approach. In this way risk can be managed on a systemic as well as an individual basis as supervisors aim to improve the risk-management at all funds rather than requiring improvements with an individual fund's risk-management. Some supervisory authorities (for example Comision Nacional del Sistema de Ahorro para el Retiro (CONSAR) in Mexico) still impose strict regulatory requirements on the risk-management framework of pension funds. However, others take a more 'prudential' approach, providing more general guidance (see Table 1). In the United Kingdom, for example, trustees are required to ensure that they have adequate internal control mechanisms in place, and a code of practice is given by the supervisory authority to trustees with the aim of providing them with practical guidance on how they might establish effective risk management processes and internal controls (see The Pensions Regulator 2006 2010).¹¹

Under a risk-based approach, it is important that supervisors not only assess the effectiveness of the overall system of internal controls, but also evaluate the controls over high-risk areas (e.g. areas with characteristics such as unusual profitability, rapid growth, geographic remoteness from the head office, new, complex, unregulated or leveraged investment products etc.). Supervisors, in evaluating the internal control systems, may choose to direct special attention to activities or situations that historically have been associated with internal control breakdowns leading to substantial losses. Certain changes in the environment should be the subject of special consideration to see whether accompanying revisions are needed in the internal control system – such as a changed operating environment; new personnel; new or revamped information systems; new technology; asset allocation to new types of investment vehicle etc. Where such risks are assessed a being systemic, such checks would be carried out on a system-wide basis (to ensure that risk is being measured and mitigated at the industry-wide as well as the individual pension fund level – see Module 3 of the IOPS Toolkit).

Working Paper No. 11 provides a checklist for supervisors when assessing the quality of pension funds' risk-management systems (see Table 2).

¹¹ For examples of guidance provided by the Australian and German authorities see (APRA 2004) and (BaFin 2009). CEIOPS have also undertaken an extensive survey of the risk-management rules applicable in European Union states (see CEIOPS 2009). Further examples of such guidance are provided in Working Paper No. 11 (IOPS 2009a).

Table 1: Regulatory Requirements for Risk-Management Architecture

	Risk management strategy	Board committees for risk management	Minimum participation in board committees	Centralised risk management function	Reporting obligations of chief risk officer (CRO)	Relationship of CRO with other functions	Compliance Officer
Netherlands	Required to be included in the business plan submitted at time of licensing	Accountability body that inter alia reviews long-term risk management	No specific requirements	Must be independent of all other departments in the pension fund	No specific requirements	No specific requirements	No specific requirements
Denmark	Board of directors required to issue risk management guidelines	No specific requirements	No specific requirements	No specific requirements	No specific requirements	No specific requirements	No specific requirements
Australia	Required for licensing and on an on-going basis; Complexity and detail depend size of fund	No specific requirements	No specific requirements	No specific requirements	No specific requirements	No specific requirements	No specific requirements
Mexico	Written policies and procedures for addressing op + and financial risk	Two board committees for op + and financial risk	Min 5 Board committee members; 1 independent/CEO/CRO	Central risk management unit (UAIR) – CRO heads ¹	To CEO, board and supervisor	Specified in detail	Compliance officer required

Source: World Bank publication, (Bruner, Hinz, Rocha, (2008)), 'Risk-based Supervision of Pension Funds: Emerging Practices and Challenges',

Note: ¹ Deals with operational and financial risks

Table 2: Risk-management System Checklist for Pension Supervisors¹

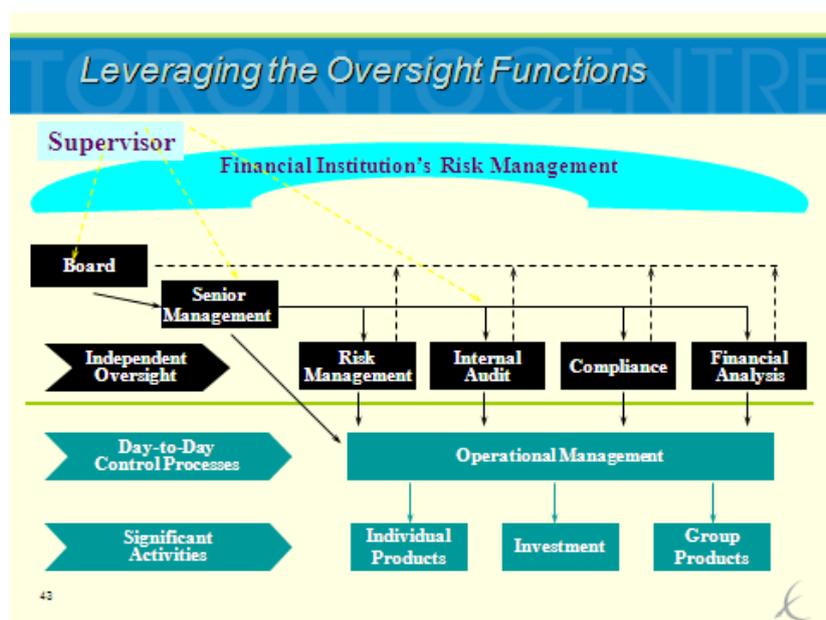
Risk-management Systems	Check Point	Details
1. Management Oversight & Culture	<i>1. Management responsibilities</i>	Are the responsibilities of the board in relation to risk-management clearly articulated and understood?
	<i>2. Division of responsibilities</i>	Are responsibilities suitably divided amongst staff, with oversight and control functions separated (<i>i.e.</i> reflecting the nature and the risks of the fund)? Is there full separation between the front and back office?
	<i>3. Management structure</i>	Is the management structured in such a way to manage risk effectively (<i>e.g.</i> dedicated committees, chief risk officer)? Are there fit and proper requirements for members of the managing board? Is there suitable oversight and accountability of the managing board? Does the managing board exercise suitable oversight of subcommittees, advisors or service providers (including auditors, actuaries and custodians)?
	<i>4. Control culture</i>	Is there an awareness and culture of control throughout the organisation? Is there a conflicts of interest policy in place? Are staff performance and compensation mechanisms regularly reviewed?
2. Strategy & Risk Assessment	<i>1. Risk-management strategy</i>	Has the board articulated a risk-management strategy which identifies risk, sets parameters and measures, monitors and controls for these risks? Is this updated regularly? Is the risk management strategy aligned with the business or institutional strategic plan? Is a suitably robust model for risk assessment used (with reliable, up-to-date, independent assumptions and data used etc.)?
	<i>2. Organisational structure</i>	Is a clear and well documented organisational structure in place?

		Is the risk-management system well integrated into the organisation structure of the organisation?
	<i>3. Investment strategy</i>	<p>Does the investment strategy cover the following?</p> <ol style="list-style-type: none"> 1. Investment objectives 2. Asset allocation 3. Diversification 4. Liquidity need 5. Valuation methodology / Pricing 6. Use and monitoring of derivatives 7. ALM targets (where appropriate) 8. Performance measurement, monitoring and benchmarking 9. Control procedures, including risk analysis/ risk tolerances / risk monitoring 10. Reporting format and frequency <p>Is a comprehensive strategy for the use of derivatives in place?</p> <p>Where appropriate, are suitable investment choices, including a default fund, offered to members?</p>
3. Control Systems	<i>1. IT systems</i>	Are the fund's IT systems suitably robust, with password controls, data back-up, system recovery mechanisms in place?
	<i>2. Monitoring systems</i>	<p>Are suitable monitoring systems in place (such as cross checking and double signatures, trails for following transactions, price and limit checks etc.)?</p> <p>Are clear limits set on transactions to be executed and positions to be taken?</p> <p>Are adequate procedures for independent determination of prices in place?</p> <p>Is frequent back testing of assumptions made in sensitivity analysis and stress tests undertaken?</p>

		Does the sophistication of the controls reflect the nature of the fund?
	<i>3. Internal audit</i>	Does the fund undertake an internal audit, and if so is it suitably empowered and independent?
	<i>4. External controls</i>	Is the external audit suitably independent and thorough? Are outsourced service providers subject to suitable monitoring?
4. Information, Reporting and Communication	<i>1. Information and reporting</i>	Is a comprehensive reporting structure in place? Are frequent and transparent reports on positions taken, limit overruns, and analysis of investment returns vs. benchmarks produced? Is the financial reporting of the fund accurate and timely? Are suitable explanations available for any variances? Are separate accounts kept for each fund/ account? Are there mechanisms in place to protect confidential information?
	<i>2. Communication</i>	Are effective channels of communication in place (upward, downward and across the organisation)? Is relevant information disclosed to all parties (including pension plan members and beneficiaries, supervisory authorities etc.)? Are there channels for adverse reporting (whistle blowing)? Is there an adequate complaints procedure?
Note: ¹ Taken from Working Paper No. 11, 'Pension Funds' Risk-management Framework: Regulation and Supervisory Oversight' (IOPS 2009a)		

In those instances where supervisors determine that the internal control system is not adequate or effective for the organisation’s specific risk profile, they should take appropriate action. This would involve communicating their concerns to the governing board of the pension fund and monitoring the actions taken to improve internal control. Where the risk was felt to be systemic and applying broadly across pension funds, the supervisory authority may react by issuing guidance notes on how they would expect risk-management systems to be improved. Other mechanisms for evaluating the quality of internal controls include using the internal audit; via a process of self assessment; using external audit services; through on-site reviews, and by undertaking dummy trades undertaken during an on-site inspection.¹²

Figure 4: Relationship between Supervisory Authority and Pension Fund’s Risk Management



Source: Toronto Centre¹

Note: ¹ *Implementing Risk-based Supervision: Leadership and Management Challenges* - presentation given by Michael Hafeman, Regional Insurance Leadership Program, April 19-24, 2009, Johannesburg, South Africa

¹² On site reviews referred to in the Toolkit are reviews which take place physically at the premises of the supervised entity.

SECTION 2: WEIGHTING RISKS- PROBABILITY AND IMPACT

Once the pension supervisory authority has established its risk focus (based on its objectives and resources), and has identified individual entity and systemic risks on a net basis (*i.e.* taking risk controls and mitigants into account), the authority then has to establish a methodology for weighting these risks. This involves establishing the probability of an adverse event and its likely impact. Quantitative and qualitative assessments will form part of the supervisor's judgement.

A. Weightings

An important aspect of the design of a risk-scoring model is the weighting assigned to different risk categories and controls. This will partly be driven by the nature of the pension system. For example, operational or legal risks may be more challenging in less developed pension systems, causing the weightings of these factors to be raised. In addition, supervisors will weight risk categories differently according to whether they are overseeing DB or DC funds.

Example: Canada



The Office of the Superintendent of Financial Institutions (OSFI) in Canada begins its risk assessment process with a review of the significant activities of a pension plan, which are broken down into 4 categories:

- Administration
- Communication to Members
- Actuarial
- Asset Management

For most federally regulated DB plans, the *Asset Management Significant Activity* will have a high impact on the Overall Net Risk rating (more so than for DC plans), and within this activity the demographic and /or liability profile are of particular importance. Likewise, the *Actuarial Significant Activity* does not apply to DC plans, but is a major driver for DB ones. The *Communications to Members Activity* receives greater weighting under DC plans.

Table 3 indicates how identified risks impact plan members and beneficiaries, sponsors and others in various pension systems.¹³ Who bears the risk will impact on the importance of the risk to the supervisory authority and the subsequent weighting of the category within the overall risk assessment.

Table 3: Impacts of Risks of Different Parties

Risk	Occupational defined benefit plans	Occupational defined contribution plans	Personal, Individual DC accounts
<i>Investment or market risk</i>	Borne by plan sponsor	Borne by plan member	Borne by plan member
<i>Counterparty default risk</i>	Not generally applicable, unless derivatives being used (e.g. for liability driven investments), in which case borne by plan sponsor	Not generally applicable (unless derivatives are being used)	Not generally applicable (unless derivatives are being used)
<i>Funding and solvency risk</i>	Borne by plan sponsor	Not applicable (unless DC plan offers guarantees in which case sponsor)	Not applicable (unless DC plan offers guarantees in which case provider)
<i>Liquidity Risk</i>	Most investments in marketable securities, so not usually significant risk, but in any event borne by plan sponsor	Not significant risk, account balances rarely large enough to pose liquidity problems	Borne by plan member, if adverse liquidity conditions create pay-out problems
<i>Mismatch risks</i>	Borne by plan sponsor	Not applicable (except that inappropriate investment profile might result in lower than expected replacement ratio, but this is "soft" risk)	Not applicable (except that inappropriate investment profile might result in lower than expected replacement ratio, but this is "soft" risk)

¹³ It should be noted that the matrix assumes a "going concern" situation, in other words, pension funds terminating with unfunded liabilities or pension accumulation funds becoming insolvent are not taken into account. In this case, many of the risks nominally borne by the plan sponsor or the pension accumulation fund will inevitably fall on the member. Pension guaranty funds and risks that might fall on them in the event of failure of a defined benefit plan are also not considered here.

<i>Actuarial Risk</i>	Borne by plan sponsor	Borne by plan member, but in individual rather than collective fashion (e.g. longevity risk, risk of outliving accumulation for scheduled draw-down pay-outs) If guarantees, borne by plan provider	Borne by plan member, but in individual rather than collective fashion (e.g. longevity risk, risk of outliving accumulation for scheduled draw-down pay-outs) If guarantees, borne by plan provider
<i>Agency Risk</i>	Borne by plan sponsor	Borne by plan member	Borne by plan member
<i>Operational Risk</i>	Borne by plan sponsor	In principle borne by pension provider (e.g. insurance company if one is involved), but if trust fund could fall on plan member	Borne by plan member
<i>IT Risk</i>	Borne by plan sponsor	In principle borne by pension provider (e.g. insurance company if one is involved), but if trust fund could fall on plan member	Borne by plan member
<i>External and strategic risk</i>	Generally borne by plan sponsor, but some external risks (such as inflation in non-indexed plan) call fall on plan member	In principle borne by pension provider (e.g. insurance company if one is involved), but if trust fund could fall in plan member	Borne by plan member
<i>Legal and Regulatory Risk</i>	Borne by plan sponsor	Borne by plan member	Borne by plan member
<i>Contagion and related party/integrity risk</i>	Borne by plan sponsor	Generally not applicable, but might be some disruption to plan member benefits if pension provider gets into trouble	Borne by plan member

Supervisors may wish to consider that risk factors with a directly measurable financial consequence should be weighted more heavily (*e.g.* the funding level in a defined benefit plan could be more critical than the plan's failure to submit a statutory return on time).

In addition, the weightings of the different risk categories and mitigants will need to be adjusted according to the nature, scale and complexity of the entity's risk being assessed. For example, a retail fund which is part of a diversified financial group and which relies heavily on the rest of the group for outsourcing may justify raised weightings in the contagion and related party risk categories. Likewise operating risk may feature highly where a fund is growing fast. Investment risk should be a specific area of concern for supervisors where exposure to risky assets (particularly those which are leveraged and/or unregulated such as hedge funds) is high.

Example: The Netherlands



The Dutch Central Bank's (De Nederlandsche Bank (DNB)) FIRM model uses templates for different types of institution, including three templates for pension funds:

- pension funds which have been fully re-insured
- pension funds which outsource nearly all their business;
- others – subdivided into pension funds that perform all functions internally and those which outsource asset management only.

The central model management team develops templates for each type of institution, assigning standard default weights denoting the importance of the different functional activities, and pre-programming risk profiles which assign default scores to the risk categories and controls.

Factors external to the pension fund may also have an influence on how different risks are weighted. The relative importance of various risks might also differ in accordance with environmental and market (systemic) factors (see Module 3 of the IOPS Toolkit). For example, longevity risk might be more significant in a developing country with rapidly improving mortality, whilst inflation rates and the liquidity and volatility of investment markets can vary significantly from one country to another—and at different times in a particular country, creating different risk-management priorities for pension funds and plans and their supervisors.

Weightings may change over time. The Retirement Benefits Authority (RBA) in Kenya is one supervisory authority which has been adapting the weightings of its model over time, reacting to

experience of using the model in practice. Some risk categories – such as counter party risk or liquidity - may need to be heightened during a financial crisis.¹⁴

Weighting - like other aspects of risk based frameworks, can be susceptible to 'gaming' by individual supervisors. A number of supervisory authorities have had experience of supervisors 'reverse engineering' their scores so that they obtain the risk ranking which they think is appropriate, and not that which is given by 'the system'. Supervisors could do sensitivity tests on their risk weightings, or back testing to try and ensure accurate and consistent approaches to weightings.

Example: Australia



The Australian Prudential Regulation Authority (APRA) have built a weighting system for individual risk categories into their PAIRS risk scoring system as follows:

PAIRS Category	Inherent Risk	Management and Control	Net Risk	Significance Weight
Board			(0-4)	%
Management			(0-4)	%
Risk Governance			(0-4)	%
Strategy and Planning	(0-4)	(0-4)	(0-4)	%
Liquidity Risk	(0-4)	(0-4)	(0-4)	%
Operational Risk	(0-4)	(0-4)	(0-4)	%
Credit Risk	(0-4)	(0-4)	(0-4)	%
Market and Investment Risk	(0-4)	(0-4)	(0-4)	%
Insurance Risk	(0-4)	(0-4)	(0-4)	%
Net Risk Total			(0-4)	100%
Coverage/ Surplus			(0-4)	%
Earnings			(0-4)	%
Access to Additional Capital			(0-4)	%
Capital Support Total			(0-4)	100%
Overall Risk of Failure			(0-4)	

Source: Australian Prudential Regulation Authority

B. Probability

Once the different risk categories and mitigants have been suitably weighted to match the structure of the pension fund, the overall riskiness of the fund is often then rated according to the probability of these risks occurring and the impact which the fund would have on the pension system in general should anything go wrong.

¹⁴ For examples of how countries responded to the financial crisis of 2008/2009 see IOPS Working Paper No. 9 (IOPS 2009b)

Assessment of the probability of an adverse event is theoretically based on the statistical concept of *conditional probability*. If certain characteristics are known historically to correlate with the occurrence of the event, the probability of the event occurring can be expressed as a function of the characteristics observed in any particular fund. While the approach is based conceptually on conditional probability, the models actually used by supervisory authorities to measure the probability of an event are typically much simpler and more subjective than would be expected under a strict conditional probability approach. They also vary widely. In some cases risks are combined additively, in other cases they are multiplied.

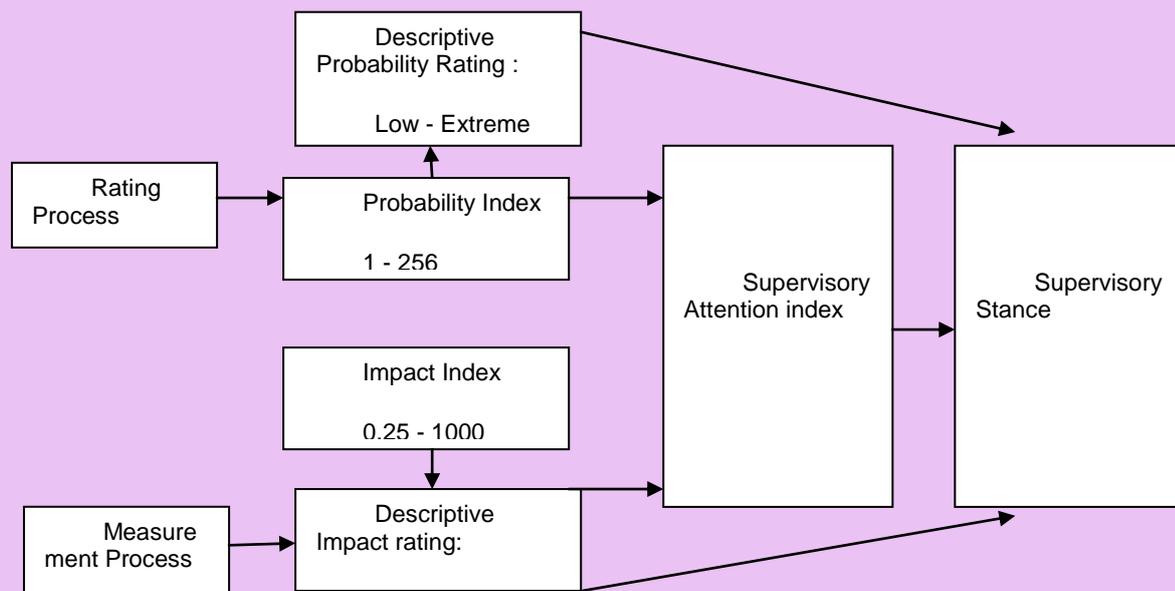
In comparing risk-based approaches to a strict conditional probability model it is interesting to note that conditional probability tends to increase non-linearly and at a declining rate as the number of uncorrelated factors increases. For example, if the unconditional probability of a DB fund's failure is 10% when poor governance is involved, and 15% when market risk is excessive, and assuming that poor governance and excessive market risk are not correlated, then the probability of failure, "conditioned" on the presence of both poor governance and excessive market risk is $(1-.1) \times (1-.15) = 23.5\%$ (not 25% and certainly not greater than 25%). The fact that most RBS probability models are either additive or multiplicative suggests that, at least implicitly, supervisors regard risk characteristics as positively correlated.

The Australian Prudential Regulation Authority (APRA)'s PAIRS systems handles the consideration of probability and impact in distinct steps— working out the magnitude of a risk a certain factor, then assigning a probability of that risk occurring, then working out the impact should this do so.

Example: Australia



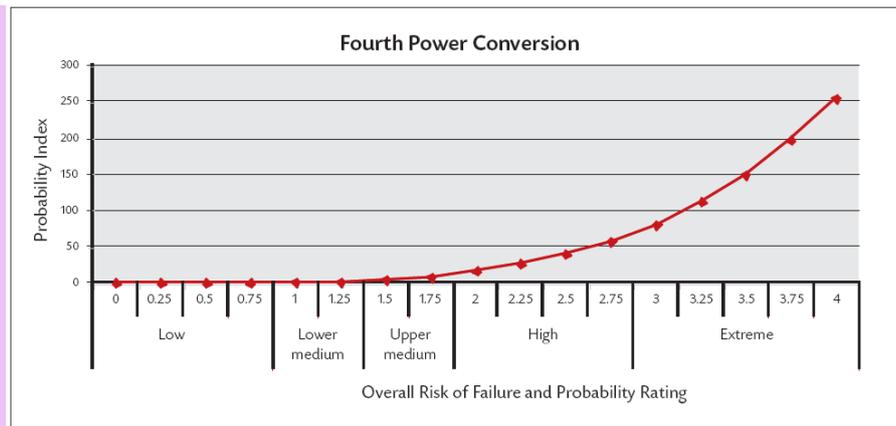
Australian Prudential Regulation Authority (APRA) Risk Probability/Impact Rating Framework



APRA converts the risk scores it assigns to each institution into a probably rating which incorporate 2 elements:

- The *Probability Rating* – a descriptive assessment of the likelihood that a regulated entity could fail. The descriptive probability scale consists of five ratings – Low, Lower Medium, Upper Medium, High and Extreme.
- The *Probability Index* – a quantitative measure of the approximate relative likelihood that a regulated entity could fail. It is a continuous curve whose function is the fourth power of the overall risk of failure.

Probability ratings rise exponentially, based on the fourth power, as the measure of financial strength falls (the fourth power calculation is an approximation and simplification of exponential formula). A net risk score of 2 will convert to a PAIRS rating of 16, while a score of 4 converts to the maximum of 256 (see chart below).



This non-linear feature mirrors the structure of commercial credit ratings (see table below) and is aimed at ensuring that the riskier entities are given particularly high profile with APRA staff and, consequently, the requisite more intense supervisory attention.

PAIRS ORF and Probability Index against Indicative External Ratings

Overall Risk of Failure		Probability Index	Indicative External Rating
Very Low	0.25	1	AAA
	0.5	1	AA+
Low	0.75	1	AA
	1.0	1	AA-
Lower Medium	1.17	2	A+
	1.33	3	A
	1.5	5	A-
Upper Medium	1.67	8	BBB+
	1.83	11	BBB
	2.0	16	BBB-
	2.25	26	BB+
High	2.5	39	BB
	2.75	57	BB-
	3.0	81	B+
Extreme	3.33	123	B
	3.67	181	B-
	4.0	256	CCC

Source: APRA (2008)

Alternatively, the FIRM framework of De Nederlandsche Bank (DNB) in the Netherlands does not evaluate probability and impact of risks separately but rather combines these into a single score. For DNB, probability means the probability of the risk event leading to a significant to high impact on the four pillars of the supervisory objectives, being solvency, liquidity, organisation and control, and integrity. This approach is based on the assumption that there is a high degree of interdependence between the probability of a risk and the magnitude of its impact. For example the probability of a market risk event leading to a major impact (e.g. a loss of 30%) is usually smaller than the probability of a market risk event leading to a minor impact (e.g. a loss of 5%). Probability is therefore assessed on the

basis of a given impact. The concept has been left implicit, as the information required for a more quantitative approach (such as probability distribution and models) is not widely available.

Some authorities adopt a simpler approach, with the risk score applied to each entity equating to the probability of problems occurring - *i.e.* as with APRA, they use a 'qualitative' or descriptive probability rating, but do not go onto the next step and convert this into a 'quantitative' probability index (as noted by DNB, the information and expertise to build and use to models will be limited in many countries).

Example: South Africa - Financial Services Board Risk ratings for Funds



Probability rating

Impact rating: *Fund Asset value*

Rating (P X I)

- 1 = < \$803 313
- 2 = > \$803 313 < \$6,7 Million
- 3 = > \$6,7 Million < \$13,4 Million
- 4 = > \$13,4 Million

Rating of administrator who administer the fund	1 = 0-40 2 = 41- 80 3 = 8 -120 4 = 121+ 4 = own administered
-------------------------------------------------	--------------------------------------------------------------------------

Number of outstanding financial statements	1 = 0 2 = 1 4 = 2+
--------------------------------------------	--------------------------

Number of outstanding valuation reports	1 = 0 2 = 1 4 = 2+
-----------------------------------------	--------------------------

Number of outstanding regulation 2(e) certificates	1 = 0 2 = 1 4 = 2+
----------------------------------------------------	--------------------------

Surplus scheme submission	1 = Yes 4 = No
---------------------------	-------------------

Early warning – information obtain from latest available financial statements

- Audit opinion	1 = Emphasis of matter 2 = Modified opinion 3 = Disclaimer 4 = Qualified
-----------------	-----------------------------------------------------------------------------------

- Bank overdraft <i>Cash at bank/current assets</i>	1 = >1<30% 2 = >30<50% 3 = >50<75%
--------------------------------------------------------	------------------------------------------

		4=>75<100%
- Arrear contributions		1= 1 month
Contributions receivable/total contributions		2= 2months
		4=>3months
-Reserve accounts		1=Total>0
		4=Total<0
- Prior year adjustments		1= No
		4=Yes
- Exceed prudent investment limits (Regulation 28)		1= >0<5%
		2=>5<15%
		3=>15<20%
		4=>20%
- Exceed 5% investment limit in a participating employer		1= No
		4=Yes
- Arrear contributions + investment in participating employer		1= No
		4 = Yes
TOTAL NET RISK RATING		

C. Impact

Impact assessments are important as they are a key determinant of a fund's relationship with the supervisory authority (*i.e.* level of monitoring it will receive). They address the question how high/low does the impact have to be before the supervisory authority will increase/reduce its oversight?

The range of impact measures is much narrower than for probability. Most authorities (*e.g.* The Australian Prudential Regulation Authority (APRA) in Australia, Financial Services Board (FSB) in South Africa) simply use the size of the fund or entity to capture the damage that would be inflicted if the adverse event occurred (*i.e.* fraud in a small fund is much less likely to damage the authority's reputation/objectives than fraud in a large fund). Judgement needs to be applied in determining how 'large' should be interpreted – with measures of numbers of active or retired members often being used as proxy. Size of assets may also be used but can be misleading (*e.g.* an underfunded DB fund may have a limited amount of assets, but this very fact should make it a high risk fund, not a lower priority one).

Example: Germany



BaFin in Germany determine the impact a crisis at a Pensionskassen or Pensionsfonds could have on the financial market exclusively from applying cut-off points. The amount of investments serves as the criteria for defining the applicable cut-off points.

- **Level 3 (high impact):** Pensionskassen or Pensionsfonds whose investments total at least EUR 10bn.
- **Level 2 (moderate impact):** Pensionskassen or Pensionsfonds whose investments total at least EUR 1bn but less than EUR 10bn.
- **Level 1 (low impact):** Pensionskassen or Pensionsfonds whose investments total less than EUR 1bn.

In individual cases an exception may be made to these established criteria (*e.g.* when the investment volume almost reaches the next cut-off point or when an entity occupies a special place in an individual market that is important for the stability of the financial sector as a whole). It is only possible to jump one cut-off point (*e.g.* from 1 to 2, or from 3 down to 2).

Any such exceptional treatment must be discussed in the risk assessment meeting and minuted. In addition, in such cases, a written report must be added to the file indicating which impact level should have been applied and why an exception was necessary.

However, such simplified measures are not always satisfactory - as the RBA in Kenya, for one, point out. Though they use the size of assets and number of members and beneficiaries as the measure of impact, problems at even small funds can have a big impact (as the failure of the nationally small but regionally important United Kingdom building society Northern Rock showed in 2007), knocking confidence in the system as a whole if they become a big story in the media. Likewise, pension funds of public bodies (say railways or municipalities) can also have more "impact" than private sector employers of the same size, as the public will demand more accountability from such bodies.

By looking beyond size, a pension supervisory authority would have a more complex, but more meaningful concept of impact. In practice this is likely to mean a few 'systemically important' pension plans (and often those are in the public sector) would be considered high impact, while the majority of the rest of the plans would not have an impact weighting assigned to them. For example, the Hungarian Financial Supervisory Authority (HFSA) in Hungary assigns *all mandatory pension funds* to the *Strong Impact* category, regardless of their size (for other types of funds, the size of membership and managed assets serves as the basis of the rating). Yet, once again, the definition of 'systematic importance' is not a simple issue.¹⁵ Determining impact thresholds is therefore an art rather than a science, which is partly

¹⁵ Systematically important financial institutions are currently being debated by the Financial Stability Board and G20 (as discussed in *Global Risk Regulator*, ISSN 1741-6620, December 2009, Volume 7, Issue 11).

determined by how much protection there is elsewhere in the system (e.g. guarantee schemes, sponsor backup, ombudsman etc.).

The relative role played by probability and impact differs across regulatory authorities. A bias towards impact means that attention is focused more on activities or events which have a relatively high impact but low probability, whilst a bias towards probability means the focus is more on high probability but relatively low impact events. The choice is a political one, and the difference can be significant. Focusing on the nature of harm can move impact measures away from an aggregate measure (how many, how much in total across an area / population) to a focus on individual impacts (*i.e.* focusing more on the nature of the impact on individuals rather than the number of individuals affected – for example focusing on particularly vulnerable individuals).¹⁶

Interestingly, impact plays no role in the Office of the Superintendent of Financial Institutions (OSFI) model used by the Federal regulator on Canada. The aggregate risk score for a pension plan is a result of the supervisors' judgement, with no detailed guidelines or formulas. Final risk scores are obtained by offsetting the aggregate risk score against the capital available to the plan. OSFI argue that impact should not be included in such decision as to give substantially different supervisory outcomes to firms on this basis would discriminate against the consumers of those firms and contrary to their legal mandate (*i.e.* that all consumers should expect equal regulatory attention).

¹⁶ See (Black 2008) p20

SECTION 3: CONSISTENCY OF SCORES

Once the supervisory authority has built its model, decided upon and weighted its inputs, a risk score can be derived for supervised entities. These risk scores then need to be checked for accuracy and consistency – which is usually done by a central risk unit within the authority.

Central vs. Individual Judgement

One of the key decisions when building a risk-scoring model is determining how much influence the individual supervisor should have in devising the risk-scoring, vs. how much central control there should be. The Australian Prudential Regulation Authority (APRA)'s PAIRS system and De Nederlandsche Bank (DNB)'s FIRM model provide an interesting contrast.

According to supervisory authorities who were the 'early adopters' of risk-based systems, such methods for centrally 'pre-populating' scores developed over time, and so now tend to be characteristic of a second or third generation risk model. Those introducing them now have benefited from this experience by introducing the technique straightaway. Pre-population can be an extremely useful way in which the centre can structure the judgement of supervisors. Indeed, some financial supervisory authorities have found that the only way to ensure that supervisors capture the external or systemic risks which it sees as relevant to a firm, for example, is to pre-populate the risk scores.

Some supervisory authorities find that the obstacles to getting information in on all the different risks from a wide number of supervisors or team, each of which is looking at a particular part, is simply so challenging that it is rarely done. For those that do try to establish a system wide view as part of their standard operations, it is easy for internal structures to proliferate. This clearly affects the speed and responsiveness of the supervisory authority, something which is particularly relevant where external market conditions are highly relevant for risk assessment and where these are changing rapidly. It is hard to have a 'real time' risk analysis if everyone in the organisation has to have a view. Yet if only a central risk unit does the evaluation the danger is that this would not be seen as valid, as it had not been validated by all the different units within the authority. There is thus a trade off between ensuring accuracy, consistency, and 'buy in' from across the authority with speed and responsiveness.¹⁷

Much depends on the internal culture within the organisation. In some authorities the supervisor can be seen as 'king' within the organisation, and as knowing the firm better than anyone else. This can make it very hard for central risk unit to get the organisation to move to a 'portfolio' approach (comparing risks across the supervised universe) rather than one led by individual risk assessments, or indeed to get supervisors to change their assessments. It can make for internal difficulties, as it is hard for supervisors to accept that 'their' firms are not as significant for the regulatory organisation, and thus of deserving as resources, as someone else's. On the other hand, where personal judgement is removed from the system supervisors may feel 'devalued'.¹⁸

¹⁷ See (Black 2008) p31

¹⁸ See (Black 2008) p31.

Examples: Australia and The Netherlands



Under the Australian PAIRS system, the individual supervisor inputs scores for risk categories and risk mitigants and decides upon the weightings these should be given depending on the institution being analysed.

Nine guidance manuals are provided to assist analysts in their assessments, outlining risk indicators for each area and all significant statutory and regulatory provisions for which compliance must be checked. Good practice and common problems are also outlined.

The PAIRS model incorporates significance weight 'reference points' for the key categories of assessment. The reference points have been established for different peer groups and are designed to reflect the significance weights of a 'typical' entity within a particular peer group, say defined benefit/hybrid funds.

At the time a supervisor makes an assessment of an individual entity in PAIRS, the reference points are available as guidance to assist with the determination of the percentage significance weights for that entity.

The reference points are centrally controlled by a dedicated team in APRA (Supervisory Framework Team). They are reviewed annually and in the interim if significant events or issues arise.

The reference points facilitate a coordinated way of increasing the importance of particular categories of assessment across one or more peer groups or the entire rated population if required. For example, if APRA considers the significance or importance of Liquidity Risk is increasing, the reference points can be centrally adjusted upwards so that supervisors make their individual assessments with the higher weights in mind. The reference points go through a number of layers of review including initial consultation with supervisory experts, ratification by the relevant industry group in APRA and final approval by APRA's Senior Executives.



By contrast DNB's FIRM model uses templates for different types of institution, including three templates for pension funds:

- pension funds which have been fully re-insured;
- pension funds which outsource nearly all their business;
- others – subdivided into pension funds that perform all functions internally and those which outsource asset management only.

The scores for the risk categories, risk mitigants and the weightings for these are already programmed into the template by the central FIRM expert team.

The individual supervisor then has to decide whether to override these scores and must record an explanation for any overrides – *i.e.* the central decision is dominant, compared with APRA's system where the individual supervisor's judgement is used to input the score (with central input merely acting as guidance).

Checking Mechanisms

The level of individual judgement in risk scoring has a consequent impact of the amount and type of central checking of a score which is then done by the supervisory authority to ensure consistency. Internal governance structures are a key issue in ensuring consistency of assessments across a large number of supervisors, and it is not always easy to get this right. In addition to training, key issues include ensuring that internal comparisons and validations are made of supervisors' assessments. Getting an 'all round view' of risks without creating overly cumbersome committee / panel structures and paralysing the organisation in procedures is a key issue.

Example: Australia



As discussed, under the Australian Prudential Regulation Authority (APRA)'s PAIRS system individual supervisors devise a risk-score for an institution. To ensure consistency these scores are then checked in various ways, including sign-off protocols, benchmarking sessions and peer reviews.

APRA began with PAIRS panels. These were panels of senior management, and they would go through two or three risk assessments in depth with the supervisors, challenging them to ensure accuracy and consistency in assessments across the organisation. However, experience showed this was a relatively cumbersome process in practice, and so APRA has moved to PAIRS forums.

This is a more group wide approach to the benchmarking process. The forum is comprised of the individual supervisors of specific institutions, Supervisory Framework Team (SFT) representatives, other supervisors and appropriate risk specialists. Between 6 and 10 entities are selected by the SFT for benchmarking. The forum discusses with the supervisors how they arrived at their scores in order to check for anomalies and discuss the criteria that supervisors are assessing against.

The forum does not have the power to change the rating; APRA considers it important that the final decision lies with the supervisors, though supervisors are likely to change the score if it has been successfully challenged in the forum.

The outcomes of each benchmarking session are circulated to participants and then more widely within APRA so that supervisors across the organisation can take into consideration the issues discussed when next making risk assessments of similar entities.

Within most supervisory authorities there is a separate set of officials responsible for the design and ongoing maintenance of the risk-based system. This unit evaluates the framework, and sets the risk parameters on which the gradings are based. The relationship of this unit with the rest of the regulatory organisation varies. It may be focused specifically on risk analysis, or have a wider role. APRA, for example, recently established a Supervisory Framework team, which is a single team across APRA dealing with all the different industries, and which is responsible not only for the maintenance and

development of the risk framework, but monitoring supervisory activity across the whole of APRA, training supervisors and producing guidance for them.

Example: The Netherlands



The Dutch Central Bank's (De Nederlandsche Bank (DNB)) FIRM model was developed by a project team comprising representatives from all supervisory divisions, as well as IT. As the project developed, input from the team was obtained via information meetings and substantive discussions on specific issues with experts from within the supervisory divisions.

One of the division directors in charge of one of the supervisory functions (currently internationally active conglomerates) has been appointed as the *owner* of the FIRM model, and is supported by the *FIRM Expert Team*, which is made up of representatives from all operational supervisory divisions.

The team is responsible for maintaining the model, providing support to users, and updating risk definitions, assessment criteria and default values in the FIRM Manual.

A *Functional Application Manager* has also been appointed for the day-to-day management of the FIRM model, covering issues such as user rights, the management existing data on institutions, adjusting default values, maintaining risk and control categories and types of key indicators and characteristics. Technical support is provided via the IT department. Staff with requests for substantive information and assistance are directed to the FIRM Manual, to the relevant member of the Expert Team or the Functional Application Manager.

For risk-scoring models to work, supervisors' own behaviour in performing the risk analysis also needs to be understood. Risk assessments are inherently judgemental, but are critical to the supervisory authority understanding of the entities it oversees and to its response. The supervisory authority therefore needs to understand how individual supervisors behave when making those judgements. Authorities which are into their second or third generation of risk-based frameworks are developing an awareness of how they need to structure the assessments to adjust for supervisors' behaviour. For example, through its validation processes one authority discovered that supervisors would over-estimate the quality of management and controls to a relatively high degree, around 30%, and moreover that this over-estimation was consistent across supervisors. Helped by the consistency of the judgements, the authority is able to adjust the basis of the calculations of the risk scores to take this over-estimation into account.¹⁹

Some authorities allow senior management in different areas to customise the model and adjust the weightings and aggregations of risk scores in their industry areas. Supervisory authorities have found

¹⁹ See (Black 2008) p23

that this has helped to engage managers; as one member of a risk team commented, 'they can play with it'. However it had the effect that the risk scores went up, as everyone thinks their area is more risky than anyone else's. Central risk units then find themselves having to 'rebase' the scores to scale them down, and readjust them between divisions in line with its own evaluations to ensure that resource allocation was not distorted.

One of the problems that authorities with some years' experience of risk-based frameworks have found is that the system can return false positives or negatives, depending on how it is designed. Where a supervisor is not sure of how to grade a particular risk, in some systems they can leave this blank. If the IT system underlying the framework automatically defaults to a low risk score, the result can be a lot of false positives. It may be that the score was left blank because it was low risk, but it may also have been left blank because the supervisor did not look at the issue or did not understand it. Authorities have met this problem in different ways. Some ensure that frameworks cannot be left blank, so one of the appointed solutions is to fill a medium score to those criteria for which there is no available information, to avoid giving weight on high or low priority which could lead to false judgements. One solution – not yet applied by any IOPS members – could be to require supervisors to state their confidence level in their assessment - although there are issues as to whether inspectors or supervisors will in fact admit to lack of confidence.²⁰

Ensuring that assessments of firms are forward looking is also a challenge. Risk assessments often only capture the risks apparent today. Some supervisory authorities include a 'direction of travel' indicator in their risk assessment: is the firm likely to improve or deteriorate over the period to the next inspection. Such judgements are built into the Hungarian authority's (Hungarian Financial Supervisory Authority's) risk assessment model, the risk matrix used by the Office of the Superintendent of Financial Institutions (OSFI) in Canada or De Nederlandsche Bank (DNB)'s FTK solvency tests, for example. However many others do not explicitly require this assessment, and have found that supervisors tend to focus on the risks as they appear now, and not on what might happen in the near future.

Supervisory authorities should retroactively test their models to validate the risk scores given and to check that these do correspond with reality and did pick up major problems. Risk based systems also entail their own risks and they need to have mechanisms for monitoring and assessing the potential risks that the frameworks themselves can create and for adjusting the framework and process accordingly. For example, the risk of myopia – where RBS becomes simply another set of boxes to be ticked, so that supervisors end up being blind to seeing risks which were not anticipated by the designers of the framework – or to something which is a problem but falls outside it. Alternatively RBS frameworks can create incentives for firms which results in them acting in a way which actually creates more risk. For example, by signalling that low impact firms will automatically receive low oversight there is little incentive for them to comply – yet non compliance of many small firms can add up.²¹

However, as many of these systems are relatively new, few examples and good practices on how this can be done are available as yet. BaFin in Germany do carry out validation of their model. This implies conducting a quality control on the data input, data output and the whole process. BaFin distinguishes between a "small validation" (plausibility check) and a "big validation" (statistical-

²⁰ See (Black 2008) p36

²¹ See (Baldwin and Black 2007), which stresses how 'really responsive regulation' needs to assess its own performance.

mathematical validation). Both kinds of validation are conducted on a regular basis, whereas under specific circumstances an extraordinary validation can be executed. Depended upon the result of the validation, it might be necessary to change the risk classification process and to customise it to the result of the validation. Triggers for validations could be external (*e.g.* changes in legislation) or internal factors (such as the introduction of a completely new rating system). Results of the validation are documented.

BIBLIOGRAPHY

- Australian Prudential Regulatory Authority (2008), '*Probability and Impact Rating System (PAIRS)*'
http://www.apra.gov.au/PAIRS/upload/PAIRS_Final_May_2008_External_Version.pdf
- Baldwin, R., Black, J.,(2007), '*Really Responsive Regulation*', LSE Law, Society and Economy Working Papers 15/2007, <https://www.lse.ac.uk/collections/law/wps/WPS15-2007BlackandBaldwin.pdf>
- Black, J., '*Risk-based Regulation: Choices, Practices and Lessons being Learned*', forthcoming OECD paper
- De Nederlandsche Bank, '*FIRM Manual*', <http://www.dnb.nl/openboek/extern/id/en/all/41-117136.html>
- IOPS (2010a), '*Revised IOPS Principles of Private Pension Supervision*',
- IOPS (2010b), '*IOPS/OECD Good Practices for Pension Funds' Risk-management Systems*'
- IOPS (2010c), '*Supervising Defined Contribution Pension Funds*' – IOPS Working Paper No. 12
- IOPS (2009a), '*Pension Funds' Risk Management Framework: Regulation and Supervisory Oversight*', IOPS Working Paper No.11, <http://www.iopsweb.org/dataoecd/31/33/43946778.pdf>
- IOPS (2009b). '*Private Pensions and Policy Responses to the Financial and Economic Crisis*', IOPS Working Paper No. 9, <http://www.iopsweb.org/dataoecd/31/0/42618315.pdf>
- IOPS (2007), '*Experiences and Challenges in Introducing Risk-based Supervision for Pension Funds*', Working Paper No. 4, <http://www.iopsweb.org/dataoecd/59/27/39210380.pdf>
- OECD (2005), '*Private Pensions OECD Classification and Glossary*'
<http://www.oecd.org/dataoecd/0/49/38356329.pdf>
- Office of the Superintendent of Financial Institutions Canada (OSFI) (2009a), '*Risk Assessment Framework for Federally Regulated Private Pensions Plans*'
http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/pension/framework/pppfrm_e.pdf
- Office of the Superintendent of Financial Institutions Canada (OSFI) (2009b), '*Overall Net Risk, Solvency, Ongoing Performance, Funding and Composite Risk Rating: Pension Supervisory Guidance Note RAF6*' http://www.osfi-bsif.gc.ca/app/DocRepository/1/eng/pension/framework/pppfrm_raf6_e.pdf
- The Pension Regulator (20010), '*Codes Related Guidance: Internal Controls*'
<http://www.thepensionsregulator.gov.uk/codes/code-related-internal-controls.aspx>
- The Pension Regulator (2006), '*Regulatory Code of Practice No.9: Internal Controls*'
<http://www.thepensionsregulator.co.uk/pdf/codeInternalFinal.pdf>

