OECD publishing

Please cite this paper as:

Stewart, F. (2010), "Pension Funds' Risk-Management Framework: Regulation and Supervisory Oversight", *OECD Working Papers on Insurance and Private Pensions*, No. 40, OECD publishing, © OECD.
doi:10.1787/5kmlcz7qq3zx-en

OECD Working Papers on Insurance and Private Pensions No. 40

Pension Funds' Risk-Management Framework

REGULATION AND SUPERVISORY OVERSIGHT

Fiona Stewart*

JEL Classification: G23, G32

*OECD, France

PENSION FUNDS' RISK-MANAGEMENT FRAMEWORK: REGULATION AND SUPERVISORY OVERSIGHT

Fiona Stewart

February 2010

OECD WORKING PAPER ON INSURANCE AND PRIVATE PENSIONS

No. 40

Financial Affairs Division, Directorate for Financial and Enterprise Affairs
Organisation for Economic Co-operation and Development
2 Rue André Pascal, Paris 75116, France
www.oecd.org/daf/fin/wp

ABSTRACT/RÉSUMÉ

Pension Funds' Risk-management Framework: Regulation and Supervisory Oversight

Drawing on the experience of the pensions and other financial sectors, this paper examines what sort of risk-management framework pension funds should have in place. Such frameworks are broken down into four main categories: management oversight and culture; strategy and risk assessment; control systems; and information and reporting. Ways in which supervisory authorities can check that such systems are operating are also considered, with a check list provided to assist pension supervisory authorities with their oversight of this important area.

JEL codes: G23, G32
Key words: Pensions, Risk-management, Risk Assessment, Internal Controls.

*****

Cadre pour la gestion des risques des fonds de pension : réglementation et surveillance

A partir de l'expérience du secteur des retraites et des autres activités financières, ce document examine le type de cadre de gestion des risques dont devraient être dotés les fonds de pension. Un tel cadre devrait reposer sur quatre grands piliers : surveillance de la gestion et culture de gestion ; stratégie et évaluation des risques ; systèmes de contrôle ; information et reporting. Ce document traite également des modalités de surveillance de ces systèmes par les instances de supervision et il contient une liste de référence à l'intention des autorités compétentes à l'égard des organismes de retraite.

Codes JEL : G23, G32
Mots clés : retraites, gestion des risques, évaluation des risques, contrôles internes.

PENSION FUNDS' RISK-MANAGEMENT FRAMEWORK: REGULATION AND SUPERVISORY OVERSIGHT

By Fiona Stewart[1]

I. Introduction

Pension supervisory authorities around the world have been following other financial sectors and moving towards a risk-based approach to pension supervision. This can be recognized as a structured process aimed at identifying the most critical risks that face each pension fund and, through a focused review by the supervisor, assessing the pension fund's management of those risks and the pension fund's financial vulnerability to potential adverse experience. A key part of a risk-based approach to pension supervision involves the supervisory authority transitioning from checking detailed compliance requirements for the operation of pension funds to reviewing the internal decision-making processes and bodies of these funds. One of the main objectives of risk-based supervision is to ensure sound risk management at the institutional level taking into account both the quality of risk management and the accuracy of the risk assessment.

As risk-based regulation often allows pension funds a freer range of investments than a strict rules-based approach (even though the supervisor may still apply some quantitative limits and asset eligibility criteria), supervisory authorities need to ensure that pension funds efficiently manage the potentially increased investment risk which they are taking on. Regulations imposing risk-management standards will therefore be required. Risk-based supervision allows much of the responsibility for risk management to rest with the individual pension fund companies themselves, while the supervisory agency verifies the quality of the fund's risk management processes and adapts its regulatory stance in response.

Risk-management frameworks can be defined as the process - effected by an organisation's board of directors, 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; and compliance with laws and regulations.[2] 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.

The importance of proper risk systems, controlling investment and other risks, has only been highlighted by the current financial and economic turmoil. Some of the decline in assets recently experienced by pension funds around the world may well have been avoided through stronger risk-

[1] Fiona Stewart is administrator in the Financial Affairs Division of the OECD's Directorate for Financial and Enterprise Affairs. This paper has also been released under the IOPS Working Paper Series, as Working Paper No. 11. The views expressed are the sole responsibility of the author and do not reflect those of her organizations. The author is solely responsible for any errors.

[2] COSO definition http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990009/PC-990009.jsp

management frameworks, as some funds appear to have been exposed to instruments whose risk profiles they did not fully understand. A sound risk framework for pension funds is essential for their prudent operation and the stability of the financial system as a whole.

Pension supervisory authorities therefore need to articulate clearly what they expect pension fund's risk-management frameworks to look like, to ensure that there are incentives for regulated entities to align their risk control mechanisms and organisational structures with these expectations, and to make sure that they have the necessary powers and authority to lead to necessary changes in supervised entities should there be a divergence.

This paper aims to outline the risk management framework which pension funds should employ, and provides guidance for pension fund regulators and supervisors on how to check that such systems are not only in place but are operating effectively.

II. Financial Sector Risk-management Requirements

Other Financial Sectors

High-level risk management requirements are laid out for entities operating in all financial sectors. For example, the Basel Committee on Banking Supervision's (BIS) *Core Principles for Effective Banking Supervision* (BIS 1997) state (in Principle 7 Risk Management Process) that: "Supervisors must be satisfied that banks and banking groups have in place a comprehensive risk management process (including Board and senior management oversight) to identify, evaluate, monitor and control or mitigate all material risks and to assess their overall capital adequacy in relation to their risk profile. These processes should be commensurate with the size and complexity of the institution."

The International Association of Insurance Supervisors (IAIS) address the issue in their *Insurance Core Principles* – ICP 10 (IAIS 2003): "The supervisory authority requires insurers to have in place internal controls that are adequate for the nature and scale of the business. The oversight and reporting systems allow the board and management to monitor and control the operations."

At the European Level, Article 43 (1) of the *Solvency II Framework Directive Proposal* (as adopted by the European Parliament's plenary session on 22 April 2009) states that: "Insurance and reinsurance undertakings shall have in place an effective risk management system comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis the risks, on an individual and an aggregated level, to which they are or could be exposed, and their interdependencies. The risk management system shall be effective and well integrated into the organizational structure and in the decision making process of the insurance or reinsurance undertaking with proper consideration of the persons who effectively run the undertaking or have other key functions."[3]

Pension Sector

OECD guidelines outline requirements regarding the risk-management systems of pension funds. The *OECD Core Principles of Occupational Pension Regulation* (OECD 2004) (2.4) state that: "Pension entities should have adequate risk control mechanisms in place to address investment, operational and governance risks, as well as internal reporting and auditing mechanism."

This requirement is echoed in the *OECD Guidelines on the Licensing of Pension Entities* (OECD 2008) (3.1). The licensing guidelines elaborate on the topic of risk-management, explaining that: "Risk

[3] It should be noted that the Solvency II Framework Directive applies purely to the insurance sector.

management procedures contribute to sound corporate practice and help to establish adequate risk measurement and management systems. These procedures include mechanisms to identify and address conflicts of interest and operational risks, such as those linked to technological failure. Specific tools are also required for the assessment and management of investment risks and other risks related to the pension fund or, where applicable, pension plan."

The Guidelines also highlight that the licensing authority should have the power to evaluate the directors and governing bodies of pension plans,[4] and to determine that appropriate corporate governance, risk management and internal controls and a code of conduct will be in place (appropriate meaning reflecting the scope and degree of sophistication of the proposed activities of the applicant). The guidelines suggest that licensing and/or supervisory authorities may provide guidance on how to meet licensing criteria: "so that better internal systems (such as risk management systems) result for the applicant."

In addition, the OECD's *Guidelines for Pension Fund Governance* (OECD 2009) address risk-based internal controls as part of the governance mechanisms: "There should be appropriate controls in place to ensure that all persons and entities with operational and oversight responsibilities act in accordance with the objectives set out in the pension entity's by-laws, statutes, contract, or trust instrument, or in documents associated with any of these, and that they comply with the law. Such controls should cover all basic organisational and administrative procedures; depending upon the scale and complexity of the plan, these controls will include performance assessment, compensation mechanisms, information systems and processes and risk management procedures." Such governance requirements are echoed in the licensing guidelines, which specifically mention codes of conduct, fit and proper requirements for members of the governing body and the functional separation between investment and settlement/bookkeeping roles.

The International Organisation of Pension Supervisors (IOPS) has *Guidelines on the Supervisory Assessment of Pension Funds* (IOPS 2008a) which state one of the objectives of the regular monitoring of pension funds as: "check risk management systems in place at the pension fund and therefore the fund's ability to handle the above risks."

National supervisory authorities also lay out risk-management requirements for pension funds in their jurisdictions, with **t**he IOPS Working Paper No. 8 (IOPS 2008c) on the '*Supervisory Oversight of Pension Fund Governance'*, containing a survey of such requirements. For example, in Australia - as described in the annex case study - the supervisory authority requires the trustees to devise a risk management framework, describing how the relevant risks are managed and monitored. In Germany, BaFin, the supervisory authority, requires that Pensionskassen and Pensionsfonds must have a proper business organisation, including sound administrative and accounting procedures appropriate to the company's business operations, must develop a risk strategy, have organisational and operational rules, and establish an appropriate internal management and control system. In the UK, Section 249A of the Pensions Act 2004 gives effect to the requirement under Article 14(1) of the European Directive 2003/41/EC (IORP Directive) that schemes should have adequate internal control mechanisms in place. Regulations state that: "The trustee or managers of an occupational pension scheme must establish and operate internal controls

[4] It should be noted that in some jurisdictions (e.g. Chile) the supervisory authority cannot remove directors or managers when they do not meet minimum requirements (though indirect enforcement via non-mandatory suggestions or recommendations may be used). An alternative mechanism to ensure proper governance is a risk scoring model that incorporates the quality of the board, and its compliance with recommendations given by the supervisory authority. The supervisor's response to a high risk entity could be as important as an intervention and, in that sense, this process would generate incentives to comply without forcing the entity to replace board members.

which are adequate for the purpose of securing that the scheme is administered and managed: a) in accordance with the scheme rules and; b) in accordance with the requirements of the law."

The IOPS Working Paper also describes how supervisory authorities in some jurisdictions also oversee the risk-management systems of external service providers. For example, in Jamaica, the governing body of a pension fund is required to review internal control policies and procedures at least annually and also regularly evaluate and report to the supervisory authority on the performance of their agents and advisers. The agents appointed by the governing body are also required by law to report to the supervisory authority on whether adequate control systems have been established to identify, monitor and manage the risk of pension plans under their management.

The paper goes on to describe how supervisory authorities may also require the governing body of a pension fund to set up a specialised, risk-management unit. In Austria, for example, Pensionskasse must establish an internal auditing unit that reports directly to the management board, and independent internal audit system is also required in Germany These audits must be carried out by experts who understand the risks that are inherent in the investments of the portfolio, with any concerns about the investment activity required to be reported to the head of investment management and the managing board. In Bulgaria, pension insurance companies are required to establish a specialised internal controls unit, appointed and dismissed by the managing body.

III. Detailed Risk-management Guidance

As one can see from above, the broad risk-management requirements laid out by different financial sectors are similar. It should therefore be of no surprise that the more detailed guidance provided by various international bodies and national supervisory agencies on how these main requirements should be met are also comparable.

Risk management systems can be broken down into four broad categories, with guidance for how to implement each aspect provided in the above recommendations:

1. Management Oversight and Culture

2. Strategy and Risk Assessment

3. Control Systems

4. Information, Reporting and Communication

	Management Oversight + Culture	**Strategy + Risk Assessment**	**Control Systems**	**Information, Reporting and Communication**
Basel Committee – Internal Controls	Management oversight + control culture -board of directors -senior management -control culture	Risk recognition and assessment	Control activities and segregation of duties Monitoring activities and correcting deficiencies	Information Communication
IAIS – ICP 10	Board of directors is ultimately responsible for establishing and maintaining an effective internal control system Oversight for market conduct activities Oversight for outsourced functions Internal controls include arrangements for delegating authority and responsibility, and the segregation of duties	Board of directors must provide suitable prudential oversight and establish a risk management system that includes setting and monitoring policies so that all major risks are identified, measured, monitored and controlled on an on-going basis	Internal and external audit, actuarial and compliance functions Accounting procedures Internal audit	Board of directors should receive regular reporting on the effectives of internal controls
IAIS – ICP 6			Applicant's risk management systems including reinsurance arrangements, internal control systems, IT systems, policies and procedures to be adequate for the nature and scale of the business in question	Information on the applicant's reporting arrangements, both internally to its own management and externally to the supervisory authority
IAIS – ICP 9	The board of directors sets out its responsibilities in accepting and committing to the specific corporate governance principles for its undertaking The board of directors establishes			

	policies and strategies, the means of attaining them, and procedures for monitoring and evaluating the progress toward them The board of directors may establish an audit committee or a risk management committee			
IAIS – ICP 18			The risk management policies and risk control system are appropriate to the complexity, size and nature of the insurer's business The risk management system monitors and controls all material risks	
IAIS – ICP 21			The risk management systems must cover the risks associated with investment activities that might affect the coverage of technical provisions and/or solvency margins (capital). The main risks include: market risk, credit risk, liquidity risk, failure in safe keeping of assets (including the risk of inadequate custodial agreements)	
CEIOPS- Risk management	Risk management strategy (objectives, risk appetite, responsibilities)	Written policies (categorization of risks, implement and facilitate appropriate risk strategy)	Processes and procedures to identify, assess, manage, monitor and report risk Own Risk and Solvency Assessment (ORSA)	Appropriate reporting procedures

CEIOPS – Internal Controls	Control environment		Control Activities Monitoring Compliance function	Information and communication
OECD – Licensing Guidelines	Fit and proper requirements and assessment for directors and governing body		Adequate risk control mechanisms to address investment, operational and governance risks, as well as internal reporting and auditing mechanism Functional separation investment and settlement roles	
OECD – Governance Guidelines	Every pension fund should have a governing body – subject to minimum suitability standards Conflicts of interest policy and appropriate controls to promote the independence and impartiality of decisions	Good governance should be risk-based - the division of responsibilities should reflect the nature and extent of the risks posed	Auditor, Actuary, Custodian should be appointed Risk-based internal controls including: regular assessment of performance and compensation mechanism; regular review of information systems, operational software, accounting and financial reporting systems; adequate risk measurement and management systems including internal audit; regular assessment of compliance systems	Use of privileged information Reporting channels between all parties involved in the administration of the fund

Management Oversight and Culture

Board Responsibilities

Management oversight and a control culture are a vital part of a functioning risk-management framework. The governing board of the pension fund is responsible for defining, implementing and improving the pension fund's risk management strategy and systems, and for establishing a high ethical standard throughout the organisation.

As well as setting up the risk-management framework, management needs to check that this is working on an on-going basis. The board should periodically discuss the effectiveness of risk-management. Identified weaknesses need to be alerted to the board as soon as possible and appropriate corrective action taken (with the board checking that any recommended improvements have been implemented). This requires systems that allow the board to receive unfiltered, honest information.

Another key risk control function that management needs to undertake is to clarify the division of responsibilities. Decision making, execution and checking functions must be assigned to different people and have suitable oversight. The OECD's *Guidelines for Pension Fund Governance* (OECD 2009) stress that good governance should be risk-based and that the division of responsibilities should reflect the nature and extent of the risks posed.

Organizational structure

As the high level requirements state, management also has to ensure that these systems are suitable and proportionate to the size and scope of the organisation. Larger entities may need committees to help the board with its tasks – such as compensation, audit, risk management committees, or a compliance committee or officer. The audit committee, for example, would be responsible for overseeing the financial reporting process and the internal control systems, as well as being the main point of contact for external auditors. Alternatively, the board may wish to create a centralized risk-management function – for example by way of appointing a Chief Risk Officer. There is some debate, certainly within the insurance sector, as to whether the risk-management function should be embedded within the structure of the organisation as a whole, or whether it should be established as a separate business unit. Whatever the structure chosen, it should reflect the nature of the fund and be clearly articulated.

To be effective, internal controls must include an organizational chart (showing who is empowered to sign for the fund and who is empowered to approve decisions etc.), and a written manual (describing the division of tasks, responsibilities, powers). The risk management system should be documented and communicated to all relevant staff members.

CEIOPS (2008)[5] outlines a well-defined organization structure for insurance companies - but which could be equally applied to pension funds - as follows:

[5] In 2009 CEIOPS published a draft level 2 advice on the system of governance, which contains some amendments to the 2008 paper. Consultation on this advice has been sought but the final paper has yet to be published. Though risk-management is a generic concept and at least parts of what CEIOPS says on the subject in the context of the Solvency II for insurers could be applied to the occupational pensions sector, it should be noted that there is no obligation required.

- it establishes and maintains effective cooperation, internal reporting and communication of information at all relevant levels with the organisation;

- it has well-defined, consistent and documented lines of responsibility across the organization;

- it ensures that members of the administrative or management bodies have sufficient professional qualifications, knowledge and experience in the relevant area of the business to give adequate assurance that they are collectively able to provide a sound and prudent management of the undertaking;

- ensures that the organisation employs personnel with the skills, knowledge and expertise necessary for the proper discharge of the responsibilities allocated to them;

- ensures all personnel are aware of the procedures for the proper discharge of their responsibilities

- establishes, implements and maintains decision-making procedures;

- ensures that any performance of multiple tasks by individuals does not and is not likely to prevent the persons concerned from discharging any particular function soundly, honestly and professionally;

- establishes information systems that produce sufficient, reliable, consistent, timely and relevant information concerning all business activities the commitments assumed and the risks to which the undertaking is exposed;

- maintains adequate and orderly records of its business and internal organization;

- safeguards the security and confidentiality of information taking account the nature of the information in question;

- introduces clear reporting lines that ensure the prompt transfer of information to all persons who need it in a way that enables them to recognise its importance;

- establishes and maintains adequate risk management compliance internal audit and actuarial functions.

Meanwhile, the OECD's *Guidelines for Pension Fund Governance* (OECD 2009) highlight that the following operational functions of pension funds should be clearly assigned: collection of contributions, record-keeping, actuarial analysis, funding and contribution policy, asset-liability management (where appropriate), investment strategies, asset management, financial education of and disclosure to plan members, regulatory compliance.

Control culture and code of conduct

The role of the board is key for ensuring that a robust risk management framework is not only in place, but also that it is applied effectively. It is the responsibility of the board of directors to develop a strong internal control culture within its organisation, a central feature of which is the establishment of systems for adequate communication of information between levels of management. Instilling a risk management culture in an entity as a whole must come from the top, with the board leading by example. Indeed it has been suggested that the most important factor in determining whether internal controls are effective is the attitude and behaviour of the senior executives who set the tone for the rest of the

organisation[6]. This ensures that risk-management is not a 'box ticking' exercise, but is truly embedded in the operations of the organisation. To install such a culture, risk-management training may need to be introduced.

The Basel Banking Committee (BIS 1998) recommends that, to instill a strong code of conduct within an organization, policies and practices that may inadvertently provide incentives or temptations for inappropriate activities should be avoided. Examples given include undue emphasis on performance targets or other operational results, particularly short-term ones that ignore longer-term risks; compensation schemes that overly depend on short-term performance; ineffective segregation of duties or other controls that could allow the misuse of resources or concealment of poor performance; and insignificant or overly onerous penalties for improper behaviour.

The Basel Committee goes on to point out that an essential element of a strong internal control system is the recognition by all employees of the need to carry out their responsibilities effectively and to communicate to the appropriate level of management any problems in operations, instances of non-compliance with the code of conduct, or other policy violations or illegal actions that are noticed. They suggest that competent employees can be secured by appropriate recruitment, ongoing training, setting motivational targets, incentive driven career paths etc. Individual mobility and transfer of responsibility at all levels may guard against problems which can arise out of routine/ habit. The OECD's governance guidelines (OECD 2009) also recommend a conflicts of interest policy (including disclosure and review procedures) and a code of conduct policy for all staff. The guidelines claim that this can best be achieved when operational procedures are contained in clearly written documentation that is made available to all relevant personnel. As the BIS point out, while having a strong risk-management culture does not guarantee that an organisation will reach its goals, the lack of such a culture provides greater opportunities for errors to go undetected or for improprieties to occur.

Strategy and Risk Assessment

Risk Strategy

A key responsibility of the board of directors of a pension fund is approving and regularly reviewing the overall strategy of the pension fund. This involves understanding the risks run; setting acceptable levels of risk; measuring, monitoring and controlling these risks; and ensuring that an adequate and effective internal control system is in place. A process for identifying risks needs to be established, with robust risk management systems being capable of quickly identifying, measuring, describing and controlling risks faced.

The management should publish a risk-management strategy which:

- identifies all material risks to the fund including operational risks (such as the risk of administrative errors, IT errors and failures, natural disasters, fraud, legal risks, outsourcing related risks and management or governance risks) and investment risks (including governance risks, market, interest rate, credit, and liquidity risks and – where appropriate – funding risks);
- assesses the likelihood and consequences of each of these;
- outlines the control mechanisms for each risk;
- highlights how they will be monitored on an on-going basis.

[6] Treadway Commission 1992 – National Commission on Fraudulent Financial Reporting (United States).

For each of the main areas it is important to assess the gross risk exposure; the effect of risk management; the net risk exposure; the volatility of results and the financial vulnerability of the organisation.

Management should review and, if necessary, update this strategy at least annually. As the high level guidance states, the strategy should reflect the nature, scale and complexity of the operations.

The Basel Committee (BIS 1998) highlight that effective risk assessment should identify and consider internal factors (such as the complexity of the organisation's structure, the quality of personnel, organisational changes and employee turnover) as well as external factors (such as fluctuating economic conditions or technological advances) that could adversely affect the achievement of the pension fund's goals. It is stressed that effective risk assessment should address both measurable and non-measurable aspects of risks, and weigh the costs of controls against the benefits they provide. The BIS point out that risks need to be evaluated to determine which are controllable and those which are not and whether the former should be accepted or managed, and how both can be mitigated. In order for risk assessment to remain effective, senior management needs to continually evaluate the risks affecting the achievement of its goals and react to changing circumstances and conditions. Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks (e.g. from financial innovation, such as new asset allocation strategies and alternative investments – as the current financial crisis demonstrates only too clearly).

Operational risk management

Operational risk is the risk resulting from inadequate or failed internal processes, people and systems or from external events. Such risks include administrative errors (for example arising from the wrongful assignment of contributions), IT errors or failures (leading to data loss or trading mistakes), as well as the more serious risk of fraud and general natural disaster risks (such as damage to buildings due to fire or natural disasters, burglary or theft of fund property). Causes include internal fraud, external fraud, employment practices, clients, products and business practices, damage to physical assets, business disruption and system failure or process management.

The management of operational risk has been receiving increased attention due to the increasing complexity of financial products, growing reliance on automated and integrated systems, online communication and outsourcing arrangements. Although the causes of operational risk are usually not financial in nature, their (indirect) consequences often are, and there is an increasing acceptance that the operational risk resulting from activities is in fact a risk that can be quantified and managed just like any other risk. Pension funds' risk management therefore needs to pay particular attention to operational risks.

An operational risk management framework should be drawn up, identifying a set of procedures, which include procedures to define, identify, assess, monitor and control operational risk. This should include a business continuity plan. Some pension funds are developing models which attempt to quantify the level of future operational risk. Quantification can be used to assess the efficiency of the fund in controlling risks and/or in providing an estimation of the capital required to absorb potential losses from operational risk events.

Investment strategy

The key part of a risk management framework for a pension fund will be its investment strategy – investment risk being the major challenge for any fund. A written investment strategy is required under OECD and CEIOPS guidance.

The *OECD Guidelines on Pension Fund Asset Management* (OECD 2006) provide further detailed guidance, including that a comprehensive investment strategy should contain the following elements:

- Investment objectives Asset allocation
- Diversification
- Liquidity need
- Valuation methodology
- Use and monitoring of derivatives
- Asset Liability Matching targets (where appropriate)
- Performance measurement, monitoring and benchmarking
- Control procedures, including risk tolerances / risk monitoring procedures
- Reporting format and frequency

The guidelines stress that the investment strategy should be consistent with legal provisions (prudent person and quantitative limits) and the objectives of the fund (i.e. with the characteristics of the liabilities, maturity of obligations, liquidity needs, risk tolerance etc,), at a minimum identifying strategic asset allocations (i.e. the long-term asset mix over the main investment categories), the performance objectives (and how these will be monitored and modified), any broad decisions regarding tactical asset allocation, security selection and trade execution. The use of internal or external investment managers should also be addressed (with an investment management agreement required for the latter), and the costs of such services monitored. In particular the guidelines note that the investment policy for pension programmes in which members make investment choices should ensure that an appropriate array of investment options, including a default option, are provided for members and that members have access to the information necessary to make investment decisions, and the investment policy should classify the investment options according to the investment risk that members bear.

The current financial crisis has only served to highlight the importance of such an investment strategy. The crisis has shown the dangers of letting pension money invest in financial markets without proper quantitative and qualitative prudential provisions against market, interest rate, credit and liquidity risk. The investment strategy should stress that pension funds should only invest in assets and instruments whose risk the pension fund concerned can properly monitor, manage and control. This is particularly the case for alternative investments seeking the higher returns promised by products such as hedge funds without fully understanding the underlying risks involved.

The IOPS '*Good Practices in Risk Management of Alternative Investments by Pension Funds'* (IOPS 2008b) also highlight specific risk-management requirements for such investments. The good practices urge that investment in these assets should fit with the pension fund's overall strategy and risk profile and that fund should regularly check that their portfolios are adequately diversified. It is stressed that pension funds should have a clear understanding of the risk characteristics of any alternative investments (which should be regularly checked). They should have confidence in the managers of any funds they invest in, and should pay particular attention to reports and valuations from fund of funds. Contract terms (lock up periods etc.) should also be checked. Risk-management systems need to pay particular attention to the valuation policies of unlisted assets during volatile market conditions. Consideration should also be given

to liquidity management programmes, which need to anticipate and plan for contractual liabilities arising from participation in infrastructure or other private asset investments.

Control Systems

At the heart of any risk-management framework are the control mechanisms – both internal and external. These should operate at every level and be an integral part of daily activities, at the top management level, as well as within each department – comprising of physical controls, checking for compliance with exposure limits, as well as systems for verification and reconciliation etc.

The core of these mechanisms is to ensure that decision making, execution and checking functions are assigned to different people and have suitable oversight. Decision making, protection of assets, accounting and control should be assigned to different staff members. This allows for controls of unintended or more sinister mistakes. Internal controls are ineffective where one person carries out two duties simultaneously (e.g. decision making and record keeping) – i.e. self-supervision needs to be avoided and cross checking mechanisms put in place.

The Basel Committee (BIS 1998) lays out various monitoring mechanisms, including senior management clarifying which personnel are responsible for which monitoring functions. They state that monitoring should be part of daily activities but also include separate periodic evaluations of the overall internal control process, with the frequency of monitoring different activities determined by the risks involved and the frequency and nature of changes occurring in the operating environment. The benefits of ongoing monitoring activities vs. separate evaluations are then considered. The former is said to offer the advantage of quickly detecting and correcting deficiencies in the system of internal control, with such monitoring said to be most effective when the system of internal control is integrated into the operating environment and produces regular reports for review. Though separate evaluations typically detect problems only after the fact, they are said to allow an organisation to take a fresh, comprehensive look at the effectiveness of the internal control system and specifically at the effectiveness of the monitoring activities. The Committee stresses that these evaluations can be done by personnel from several different areas, including the business function itself, financial control and internal audit, and that separate evaluations of the internal control system often take the form of self-assessments when persons responsible for a particular function determine the effectiveness of controls for their activities. The documentation and the results of the evaluations are then reviewed by senior management. The Committee emphasize that all levels of review should be adequately documented and reported on a timely basis to the appropriate level of management.

IT Systems

With all types of financial services now highly dependent on technology, internal controls are needed to verify the security of the IT systems. IT security risks could be defined as security risk relating to all potential confidentiality, integrity, availability and accountability compromises of an institution's IT resources. Such IT security risks include the concentration of data, which can weaken the security of information and the use of complex applications which can result in the repetition of problems. Risks of error, fraud, negligence, and chance mishaps (such as system crashes) all need to be protected against. Equally important is data integrity as a mitigating factor against risks such as incorrect benefit payment.

Controls are needed to ensure the physical and logistical security of data, including the protection of files and software. An audit trail is also required (i.e. written procedures allowing for chronologically reconstituting transactions, justifying any transaction by using a source text to follow an unbroken trail to and from the financial statement and explaining the changes in balance from one statement of account to

another by showing what transactions have been performed). The information processes, operational software systems, and accounting and financial reporting systems will need to be regularly reviewed.

Controls over information systems and technology should include both general and application controls. General controls are controls over computer systems (for example, mainframe, client/server, and end-user workstations) and ensure their continued, proper operation. General controls include in-house back-up and recovery procedures, software development and acquisition policies, maintenance (change control) procedures, and physical/logical access security controls. Application controls are computerised steps within software applications and other manual procedures that control the processing of transactions and business activities, including, for example, edit checks and specific logical access controls unique to a business system. Necessary protection measures will include:

- IT security requirements (data protection, firewalls)
- Data backup
- System recovery
- Password controls

In addition to the risks and controls above, inherent risks exist that are associated with the loss or extended disruption of services caused by factors beyond the organisation's control. This potential requires contingency plans using an alternate off-site facility, including the recovery of critical systems supported by an external service provider. Business resumption plans must be periodically tested to ensure the plan's functionality in the event of an unexpected disaster.

Monitoring systems

One goal of risk management is to certify that the policies and strategy of the managing board of any organisation are applied correctly. As the high level guidance points out, the more complex the organisation the more rigorous these will have to be. Risk-management frameworks should ensure that transactions have been carried out by the persons assigned, in ways authorized by the managing board (delegation of signatures, division of tasks and control procedures etc.). Decision making (or authorizing decisions), protection of assets, accounting and control should be assigned to different staff members. Such checks will include:

- Segregation of duties (e.g. front/ middle/ back office)
- Cross checking
- Dual control of assets
- Double signatures
- Decision making limits/ authorizations
- Reconciliation procedures

- Compliance systems / officer[7]

- Monitoring of third party / outsourcing agreements

Internal audit[8]

A key element of the risk-management and monitoring framework is the internal audit – the nature and scope of which should be appropriate to the operations of the pension fund. The IAIS (IAIS 2006) point out that it is critical that the internal audit function is independent from the day-to-day operations of the pension fund. Responsibilities of the internal audit include ensuring compliance with all applicable policies and procedures and reviewing whether the fund's policies, practices and controls remain sufficient and appropriate.

The IAIS stress that the internal audit must have unrestricted access to all departments and information; be suitably independent (reporting to the board); have sufficient weight and resources to carry out its task. In terms of good practice, it is pointed out that the internal audit should issue reports directly to the board of directors or its audit committee, and to senior management, thereby providing unbiased information about operational activities. It is suggested that further independence can be reinforced by the board having such matters as the compensation or budgeted resources of the internal audit determined by the board or the highest levels of management rather than by managers who are affected by the work of the internal auditors. The IAIS also stress that, due to the important nature of this function, the internal audit must be staffed with competent, well trained individuals who have a clear understanding of their role and responsibilities.

Performance measurement and compensation mechanisms

According to the OECD's *Governance Guidelines* (OECD 2009), the performance of the persons and entities involved in the operation and oversight of the pension fund will need to be assessed regularly, particularly where the governing body is also a commercial institution. Mechanisms are needed to assess regularly the performance of the pension entity's internal staff, as well as external service providers (e.g. those providing consultancy, actuarial analysis, asset management, custody another services). Objective performance measures should be established for all the persons and entities involved in the administration of the pension fund. For example, appropriate benchmarks should be established for external asset managers. Performance should be regularly evaluated against the performance measures and results should be reported to the relevant decision maker, and, where appropriate, to the supervisory board, the supervisory authority, and the pension fund members and beneficiaries. The benchmarks should be reviewed regularly also to ensure their consistency with the pension fund objectives (e.g. the investment strategy).

The OECD Guidelines (and the Basel Committee) also point out that risk management needs to consider compensation mechanisms, in order to ensure that they provide the correct incentives for those responsible for the operation and oversight of the pension fund. Appropriate compensation can provide the right incentives for good performance. The OECD Guidelines suggest that the establishment of a

[7] As described by the IAIS, the compliance function advises management on compliance with laws and regulations and may also produce assessments of the possible impact of any significant changes in the legal environment on the operations of the undertaking concerned the identification and assessment of compliance risk. The compliance role should not conflict with other obligations and should be able to access records and communicate freely to carry out its role.

[8] Detailed guidance on the internal audit of insurance companies is provided by the IAIS (IAIS 2006) ICP 10 Internal Control.

compensation committee and chairperson may optimise the process of evaluating the compensation of those responsible for the operation and oversight of the pension fund, such as asset managers, custodians, actuaries, as well as the members of the governing body. Legislation in Chile goes one step further as a mechanism exists for the affiliates of a pension plan to obtain remedy to economic damages which have arisen as a consequence of inadequate administration of their pension fund by their Pension Fund Administrator (AFP). The law provides this duty of compensation (loss of return) in case the AFP breaches either the obligations imposed on itself by the law or the instructions of its affiliates.

The OECD guidelines go on to warn that the compensation policy of sales forces of pension plan providers may also warrant close scrutiny by the governing body, since these costs can reduce pension benefits significantly. There is a risk also that sales staff may not act in the best interest of plan members and beneficiaries, offering products that are not suitable for certain individuals. The governing body should therefore ensure that the remuneration structure for sales staff does not create distorted incentives or and lead to ill-advised decisions by consumers.

The OECD guidelines recommend that objective performance measures should be established for all the persons and entities involved in the administration of the pension fund. For example, appropriate benchmarks should be established for external asset managers. Performance should be regularly evaluated against the performance measures and results should be reported to the relevant decision maker, and, where appropriate, to the supervisory board, the supervisory authority, and the pension fund members and beneficiaries. The benchmarks should be reviewed regularly also to ensure their consistency with the pension fund objectives (e.g. the investment strategy).

Meanwhile a compensation committee may optimize the process of evaluating the compensation of those responsible for the operation and oversight of the pension fund, such as asset managers, custodians, actuaries, as well as the members of the governing body. The compensation of sales forces of pension plan providers may warrant particularly close scrutiny.

External Controls

In addition to – and working with – the internal control mechanisms, external parties also have a role to play in the risk-management of a pension system. Such mechanisms include:

- Reports of the supervisory board
- Asset custody
- Actuarial reports
- External Audit

The OECD's governance guidelines (OECD 2009) outline the role of auditors, actuaries and custodians, highlighting the whistle blowing responsibilities of these parties.

The Basel Committee (BIS 1998) stress that although external auditors are not, by definition, part of an organization and therefore, are not part of its internal control system, they have an important impact on the quality of risk management through their audit activities. External auditors can influence risk management systems in various ways, including through discussions with management and recommendations for improvement, which provide important feedback on the effectiveness of the internal control system. The Committee points out that external auditors have to obtain an understanding of the internal control system in order to assess the extent to which they can rely on the system in determining the

nature, timing and scope of their own audit procedures. Though the nature and extent of the external audit will vary by country the Committee underline that it is generally expected that material weaknesses identified by the auditors would be reported to management in confidential management letters and, in many countries, to the supervisory authority, and that external auditors may be subject to special supervisory requirements that specify the way that they evaluate and report on internal controls.

It should be noted that in some countries (e.g. in Chile) the relationship between pension plan administrators and the external service providers with whom they sign contracts is increasingly important (for example the foreign investment of pension funds requires not only financial expertise but also a comprehensive legal understanding of contracts under different jurisdictions). An evaluation of the capacity of a pension fund administrator to establish adequate contracts with different financial institutions - such as custodians, brokers/ dealer, central counterparties - should therefore be highlighted in any risk-assessment.

Information, Reporting Communication

Information and reporting

Proper information flows are vital for risk-management frameworks to operate properly. Adequate and comprehensive internal financial, operational and compliance data and external market information is needed, with all information required to be reliable, timely, accessible and consistent. A policy also needs to be in place to ensure that confidential information is treated appropriately.

Efficient reporting is an important part of any risk-management framework. Information needs to be released to the correct parties in an understandable format, and with due frequency. Separate records should be kept for each pension fund or account.

Communication

Effective channels of communication are required so that everyone understands their responsibilities and to make sure that relevant information is reaching the appropriate personnel. Without effective communication, information is useless. The organisational structure should facilitate an adequate flow of information - upward, downward and across the organisation. A structure that facilitates this flow ensures that information flows upward so that the board of directors and senior management are aware of the business risks and the operating performance. Information flowing down through an organisation ensures that objectives, strategies, and expectations, as well as its established policies and procedures, are communicated to lower level management and operations personnel. Communication across the organisation is necessary to ensure that information that one division or department knows can be shared with other affected divisions or department.

Communication lines should encourage adverse reporting (whistle blowing) – particularly when flowing upwards. Internal control deficiencies, or ineffectively controlled risks, should be reported to the appropriate person(s) as soon as they are identified, with serious matters reported to senior management and the board of directors. Once reported, it is important that management corrects the deficiencies on a timely basis. The internal auditors should conduct follow-up reviews or other appropriate forms of monitoring, and immediately inform senior management or the board of any uncorrected deficiencies. In order to ensure that all deficiencies are addressed in a timely manner, senior management should be responsible for establishing a system to track internal control weaknesses and actions taken to rectify them.

IV. Supervisory Oversight of Pension Funds' Risk-management Frameworks

Given the enhanced role required of a pension fund's risk-management framework under a risk-based approach to supervision, supervisory authorities will need to provide guidance on what they expect pension fund's risk management frameworks to look like. The IOPS Working Paper No. 8 (IOPS 2008c), *'Supervisory Oversight of Pension Fund Governance'*, highlights that for non-professional governing bodies, one of the best supervisory approaches is to equip them with necessary skills and knowledge of internal controls. In the UK, 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. Examples of guidance provided by the UK and Australian supervisory bodies are provided in the following case studies.

The *IOPS Principles of Private Pension Supervision* (IOPS 2006) stress that supervisors should have a risk-based approach. It is important that they not only assess the effectiveness of the overall system of internal controls, but also evaluate the controls over high-risk areas. 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 senior management and monitoring what actions is taken to improve internal control. 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 etc.

To evaluate the quality of internal controls, supervisors can take a number of approaches:

Internal Audit

Supervisors can evaluate the work of the internal audit department through review of its work papers, including the methodology used to identify, measure, monitor and control risk. If satisfied with the quality of the internal audit department's work, supervisors can use the reports of internal auditors as a primary mechanism for identifying control problems, or for identifying areas of potential risk that the auditors have not recently reviewed. The less the supervisor can rely on the internal (or external) audit, the more in-depth their own investigation will have to be.

Self Assessment

Some supervisors may use a self-assessment process, in which the pension fund's management reviews the risk management framework and certifies to the supervisor that its controls are adequate. The supervisory authority would then check whether the self-assessment of the managing board is accurate. IOPS Working Paper No. 8 (IOPS 2008c) notes that supervisory authorities would generally assess the internal control structure and mechanism of the governing body during the licensing process (e.g. Hungary, Poland, South Africa and Turkey). For example, in Thailand, as part of the licensing criteria, the SEC has to ensure that the governing body has in place proper internal control system which consists of but not limited to operation manuals, check and balance system, complaint-handling process, control environment and activities, information and communication, monitoring and risk assessment.

External Audit

Other supervisors may require periodic external audits of key areas, where the supervisor defines the scope. Supervisors should take note of the external auditors' observations and recommendations regarding

the effectiveness of internal controls and determine that management and the board of directors have satisfactorily addressed the concerns and recommendations expressed by the external auditors. The level and nature of control problems found by auditors should be factored into supervisors' evaluation of the effectiveness of the internal controls. In some jurisdictions, if the supervisory authority does not have expertise in particular areas to conduct in-depth analysis of the internal control of the governing body, it may engage the services of independent, external experts. The skills of the external experts may strengthen the capabilities of supervisory authorities.

On-site Inspections

Supervisors may combine one or more of the above techniques with their own on-site reviews or examinations of internal controls. On-site inspections should include an assessment of a pension fund's risk management architecture, and indeed may be the only way to confirm the quality of the control systems. A full assessment of a risk management system will require several stages. First the supervisor needs to understand the system which is in place (via studying manuals, internal audit reports etc.). The supervisor will then need to establish whether the systems actually exist in practice. This could be done via a questionnaire send to key operational staff (asking for specific details on how certain checks are undertaken, for example).

Supervisors are in effect acting as 'super external auditors' – with additional scope and powers to their investigations to normal internal and external checks. For example, their investigation is universal, seeking to establish an overall picture of the risk management architecture, where as an internal operational audit may only focus on one division. Also the conclusions of the supervisor will be directed to the board, and any recommendations will be binding.

IOPS Working Paper No. 8 (IOPS 2008c) explains how on-going monitoring is often needed to ensure that the parties involved in pension fund administration implement and practise the rules and procedures in respect of internal controls. The paper points out that it is a common practice for supervisory authorities to conduct on-site and off-site inspections of the internal control system of the governing body and/or other service providers.

For example, in Hong Kong, the supervisory authority regularly reviews the internal control reports submitted by the trustees and periodically conducts on-site inspections on the trustees' operations to ensure adequacy of internal controls. Meanwhile in Turkey, adequacy of internal controls is checked during on-site inspections by utilizing the feedback gathered from off-site supervision. In Jamaica, during on-site examinations, the internal control environment is evaluated to determine the existence, adequacy and effectiveness of internal controls. Documents, including internal and external audit reports, operational policies and procedures and job descriptions, are examined. In Macedonia, MAPAS conducts regular on-site audits on the key areas of internal controls of the governing body, e.g. internal procedures, decision-making process and major control points. A comprehensive on-site inspection is performed annually, while partial on-site inspections may be conducted more frequently if any internal control weaknesses have been identified. In the Netherlands, the DNB actively performs supervision over the pension fund's system of internal control, e.g. during on-site visits. The Pension Act requires pension funds to regularly perform a continuity analysis that provides insight into its long-term financial position. DNB reviews these continuity analyses, based on a number of criteria laid down in specific guidelines.

The paper goes on to explain how some supervisory authorities may focus their supervisory oversight on the internal control unit of the governing body. In Hungary, for example, the HFSA either supervises the activities of internal controllers during on-site inspection or communicates with them in the course of daily supervision. The HFSA may also contract the services of an expert, in certain cases, to carry out inspections. In Poland, during on-site inspections, the supervisory authority studies the documents

produced by the internal control unit, including its work plans and internal control reports, to assess whether or not the governing body has complied with relevant law and regulations. Among others, the investment activities of fund managers may be inspected to ensure that no insider trading activities have taken place.

The IOPS *Supervisory Assessment Guidelines* (IOPS 2008a) recommend the following when evaluating the management and internal control system of a pension fund:

- review of the minutes of the meeting of the governing body of the pension fund, and detailed examination of the auditor's and actuary's reports;
- evaluation of the management's capacity to run the fund, their efficiency, and their ability to acknowledge and correct their management mistakes (especially after management changes);
- audit of selected internal procedures and risk control systems, (including internal audit, reporting, monitoring and IT systems), in order to assess the relevance and robustness of these internal controls and the fund's approach to risk management;
- examination of the accounting procedures in order to know whether the financial and statistical information periodically sent to the supervisory authority is reliable or not, and in compliance with the regulations;
- examination of the governance structure and governance mechanisms of the pension fund (including the segregation between operational and oversight responsibilities).

Dummy Trades

Supervisors may ask for 'dummy trades' to be executed on the systems to see how they operate. The less sure the supervisor is of the reliability of the risk management system, the more tests and investigation will need to be carried out. The Basel Committee (BIS 1998) suggest that an appropriate level of transaction testing should be performed to verify:

- the adequacy of, and adherence to, internal policies, procedures and limits;
- the accuracy and completeness of management reports and financial records; and
- the reliability (i.e., whether it functions as management intends) of specific controls identified as key to the internal control element being assessed.

Assessment of service providers' risk-controls

IOPS Working Paper No. 8 (IOPS 2008c) points out that the quality of the internal control systems of pension fund service providers may pose a threat to the funds and thus the interests of plan members and beneficiaries. The governing body is therefore in some cases required to ensure that their service providers (particularly those involved in investment management) have set up appropriate internal control systems. The report points out that supervisory authorities may have to monitor the internal control systems of pension fund service providers which perform important functions such as investment management. Such monitoring could be performed either by the supervisory authority itself or through the governing bodies of the pension funds. For example, in Thailand the governing body of a fund is required to include in its contract with the service providers certain clauses which would enable the supervisory authority – the SEC - to carry out inspections to the service providers as and when necessary. In Australia, the supervisory

authority is developing a programme for on-site review of entities in the two major categories of service providers i.e. the administrators and custodians.

ANNEX 1: PENSION FUND RISK-MANAGEMENT CHECKLIST

The following check list – built on OECD, IAIS and other guidance - provides more details for what a pension supervisor may look for to determine whether the key aspects of any risk management framework are in place at the pension fund which they are examining.

It should be noted that risk-management procedures are becoming increasingly cumbersome and sophisticated. Therefore, though they must be adequate, these controls need to be appropriate to the size, scale etc. of the organisation, there needs to be some cost benefit analysis. In entities with a limited number of staff some may have to take on multiple duties, but the board needs to then manage potential conflicts of interest with additional controls (and audit function must always remain independent). The *OECD Guidelines for Pension Fund Governance* (OECD 2009) also highlight that the scope and complexity of internal control measures should be 'risk-based' and will vary according to the type and size of pension plan, fund and entity and the type and extent of risks faced.

This is meant to be a general guide for supervisory authorities, to be used in assessing their own supervisory methods and procedures. Though the exact approach taken by the authority will depend on a host of factors (including their on-site and off-site supervisory techniques) the principles set out can be used by all.

The checklist could also be used by pension funds looking to conduct their own self assessments.

Risk-management Architecture	Check Point	Details
1. Management Oversight & Culture	*1. Management responsibilities*	Are the responsibilities of the board in relation to risk-management clearly articulated and understood?
	2. Division of responsibilities	Are responsibilities suitably divided amongst staff, with oversight and control functions separated (i.e. reflecting the nature and the risks of the fund)? Is there full separation between the front and back office?
	3. Management structure	Is the management structured in such a way to manage risk effectively (e.g. 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 body exercise suitable oversight of subcommittees, advisors or service providers (including auditors, actuaries and custodians)?
	4. Control culture	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*	*1. Risk-management strategy*	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.)?
	2. Organisational structure	Is a clear and well documented organisational structure in place? Is the risk-management system well integrated into the organisation structure of the organisation?
	3. Investment strategy	Does the investment strategy cover the following?

		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 Is a comprehensive strategy for the use of derivatives in place? Where appropriate, are suitable investment choices, including a default fund, offered to members?
3. Control Systems	*1. IT systems*	Are the fund's IT systems suitably robust, with password controls, data back-up, system recovery mechanisms in place?
	2. Monitoring systems	Are suitable monitoring systems in place (such as cross checking and double signatures, trails for following transactions, price and limit checks etc.)? Are clear limits set on transactions to be executed and positions to be taken? Are adequate procedures for independent determination of prices in place? Is frequent back testing of assumptions made in sensitivity analysis and stress tests undertaken/ Does the sophistication of the controls reflect the nature of the fund?
	3. Internal audit	Does the fund undertake an internal audit, and if so is it suitably empowered and independent?
	4. External controls	Is the external audit suitably independent and thorough? Are outsourced service providers subject to suitable monitoring?

4. Information, Reporting and Communication?	*1. Information and reporting*	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?
	2.Communication	Are effective channels of communication in place (upward, downward and across the organization)? 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?

ANNEX II: PENSION FUND RISK-MANAGEMENT REGULATION AND SUPERVISION IN SELECTED COUNTRIES

1. Regulatory Requirements for Risk Management Architecture[9]

	Risk Management Plan Strategy	**Board Committees for Risk Management**	**Minimum Participation in Board Committees**	**Centralized Risk Management Functions**	**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: Complexity and detail depend on fund size	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 operational and financial risk	Two Board Committees for operational and financial risk	Board Committees must have at least 5 members: 3 Board members, of which one independent, the CEO and the CRO	Central risk management unit (UAIR) dealing with operational and financial risks and headed by Chief Risk Officer (CRO)	To CEO, Board and Supervisor	Specified in detail	Compliance Officer required

[9] This section is taken from the World Bank publication on risk-based supervision (Brunner et al 2008).

Australia, Denmark, and the Netherlands impose some requirements on risk management as part of licensing or initial registration procedures. This includes the elaboration of a risk management plan or risk management guidelines. These requirements are not very detailed, with the supervisors allowing for differences depending on the size of the institution. These countries do not seem to impose specific regulatory requirements on the internal risk management architecture, although Dutch funds must have an internal body reviewing long term risk management, as well as independent risk management functions.

In Australia there are no specific requirements in legislation or regulations for establishing board committees, minimum participation in board committees, a centralised risk management function, reporting obligations of chief risk officer and that official's relationship with other functions (or indeed to prescribe such an office), or a compliance officer. However, the Risk Management Strategy and Plan (see following country case study) must set out the arrangements for internal oversight, implementation and reporting in relation to management of material risks. These arrangements would be expected to consider and document the need for and/or operation of the committees and risk management functions noted.

Alternatively, Mexican supervisors have followed a different approach, issuing a direct regulation that specifies in detail all the elements of the internal risk management architecture. All pension funds must have two Board committees dedicated to risk management, one focused on operational risk and the other on financial risk. Each committee must have at least five members, of which are three Board members. At least one of the Board members must be independent. The other members are the Chief Executive Officer (CEO) and the Chief Risk Officer (CRO). The CRO heads an independent and central risk management unit (UAIR), addressing both operational and financial risks, and must report to the Board, the CEO and the supervisor. The regulation specifies in detail the duties and obligations of the CRO, including the interactions with other key executives such as the Chief Investment Officer. The regulation also requires the presence of a compliance officer ensuring observance of all the regulations.

It is difficult to make a comparison of the effectiveness of these two approaches, because Australian, Danish, and Dutch supervisors may also induce institutions to adopt sound risk management practices through their risk scoring models. As explained in more detail below, risk scoring models measure the exposure of institutions to risk and their capacity to manage these risks. This capacity is assessed in some detail, entailing the assessment of the quality of very specific elements of risk management, procedures, and control. Institutions which receive low scores are typically subject to more intensive supervision and are pressed to remedy their deficiencies.

The Australian Prudential Regulatory Authority (APRA) introduced a guidance note on risk management to further explain the risk management requirements inserted into the legislation in the context of a comprehensive re-licensing program that has resulted in a sharp reduction in the number of institutions. Its supervisors report that several institutions could not demonstrate their capacity to prepare or implement a coherent risk management plan during the re-licensing process. The Australian experience suggests that pension supervisors probably need to consider a combination of tools to ensure the introduction of sound risk management practices in all institutions, while also providing the necessary flexibility for institutions of different sizes.

The Mexican approach can only be implemented in systems with fewer and larger pension funds. The Mexican approach merits consideration by countries with similar systems, although its effectiveness would need to be assessed in the coming years. One of the issues that would need to be examined is whether the approach works well across different institutions, including institutions which are part of financial conglomerates owned by parent companies abroad – a very common situation in systems like the Chilean and Mexican.

2. Australia[10]

Legislation in Australia requires pension funds to establish a two-tier risk management framework involving a Risk Management Strategy (RMS), which primarily relates to trustee-specific risks, and a Risk Management Plan (RMP) relating to operational risks. These are assessed as part of the trustee licensing process.

The RMS must set out procedures to identify, monitor and manage risk associated with:

- governance and decision making;
- outsourcing;
- any changes to the licensee law;
- potential fraud and theft.

The RMP deals with operational risks including:

- investment strategy;
- financial position;
- outsourcing.

All 'material' risks must be addressed, including an assessment of the likelihood and consequence of each and arrangements for internal oversight, implementation and reporting in relation to their management is required. Circumstances in which an audit of these risks is to be undertaken must also be outlined and the RMS must be kept up to date (reviewed at least annually), with modifications being required if it is found to no longer comply with legislation

The requirements do not differ according to the type of superannuation fund, though APRA expect the risk management framework to reflect the nature, scale and complexity of the operations. Indeed APRA caution against trustees adopting generic frameworks and documentation which do not take into account the particular nature of the business.

APRA believe that the risk management framework should be developed within the context of the trustee's business plan.

APRA's guidance note outlines the following elements as part of the RMS and RMP:

- ***Risk identification and assessment*:** considering specific governance risks; investment risk; liquidity; operational risk; outsourcing risk; agency risk; fraud risk; market and counterparty risks; insurance risk and external risks (legal changes etc.). Once risks have been identified they may be recorded in a risk register or an appropriate data base, with the trustee rating the likelihood and consequence of each. Scenario analyses and stress testing may also be used.

[10] This case study is taken from APRA (2004)

- ***Risk treatment***: controls mitigating each risk should be identified, and a qualitative assessment of the residual risk remaining made, with these then ranked. Risks should be accepted, mitigated, transferred or avoided.

- ***Internal oversight, implementation and reporting:*** trustees should implement adequate communication and reporting systems and ensure information flows between parties. A process of regular internal risk reporting to the trustee should be established. The trustee is also responsible for ensuring that a strong risk management culture is adopted, with the following recommended as ways to ensure compliance with risk management policies and procedures:

  - clearly defined management responsibilities;

  - adequate segregation of duties;

  - establishing a risk committee (or similar) to set the strategy for and review the risk management framework;

  - instituting risk controls for each department/division, including limits on market and counterparty risk;

  - having appropriate selection and security checks for all staff;

  - incorporating discussion of risk management policies into staff induction and training and/or; use of external consultants to assess risk management frameworks.

APRA's ongoing supervision, both on-site and off-site, involves the review of the risk management framework and its functioning and effectiveness. This approach is underpinned by legislation, for example if a risk management plan is updated to reflect new business operations or a changed view of a particular risk factor, the updated plan must be submitted to APRA. Plans must be reviewed periodically. Where APRA assesses a risk management strategy or plan to be inadequate, APRA requires the trustee to amend both the written policy and its practices.

In the context of its risk-based supervision approach, APRA's assessment of an institution's risk governance is a major determinant of the supervision stance adopted in respect of the institution. An institution would be rated as having a strong risk governance approach if, among other things,

- The role and responsibilities of the Board is clear.

- There is strong evidence demonstrating that the Board provides clear direction and leadership for the entity and that they take their obligations to their beneficiaries seriously.

- There is strong evidence that the Board is functioning effectively in key areas.

- A robust Risk Management Framework (RMF) is in place, is regularly reviewed and exceeds minimum requirements in key areas.

- The Committee structure is well established and there is strong evidence that Committees are functioning effectively.

- An audit Committee is well established, exceeds prudential requirements and there is strong evidence that it is functioning effectively.

- The performance of Board and Committees is regularly reviewed.

- Strong internal audit, external audit and, where applicable, actuarial functions exist. There are clearly independent, high quality staff, adequately resourced and effective.

- There is a strong compliance framework/ function that is independent, adequately resourced, with high quality staff, clear identification and resolution processes.

3. Brazil[11]

In recent years, the modernization and professionalization of the private pension system in Brazil have been accompanied by an increase in the supervision of closed, private pension entities by the National Secretariat for Pension Funds (SPC). The system regulation has been improved, with the incorporation of international best practices, especially those related to risk-based supervision.

The CGPC Resolution No. 13 was published on October 1, 2004, standardizing the rules and governance practices, management and internal controls to be observed by closed private pension entities (EFPC). This Resolution enabled the pension supervisory body to align itself with guidelines issued by other supervisory bodies overseeing the financial system, as well as regulatory good practices adopted around the world. In its articles, the Resolution refers to some rules that the EFPC should adopt in developing its activities, especially those related to environmental control, risk identification, control activities, monitoring activities, information and communication.

Since the regulatory and supervisory body became concerned with the implementation of effective internal controls by and EFPC, the Resolution CGPC No 13 reinforced the need for members of the deliberative and fiscal council to have necessary abilities, experience and to be constantly updated in regard to their duties, giving them the prerogative to hire auditing companies to evaluate the internal controls of the pension fund. Going forward, the Resolution requires the fiscal council to prepare an internal control report every six months regarding, among other things, the investment policies, the management of plan assets, actuarial assumptions and the execution of the budget.

The resolution also ascribed to the pension fund, and its management and governance boards (if they exist), the responsibility to develop a culture that emphasizes and demonstrates the importance of internal controls at all hierarchical levels. These controls, in turn, must be appropriate to the size, complexity and risks associated to the benefit plans administered by pension funds.

Finally, this Resolution advises the funds to establish a *Code* of *Ethics and Conduct* and to produce a governance manual. The Resolution also encourages operational independence between the statutory bodies, avoiding conflicts of interest (and instead always working towards the common good and goals of the pension fund).

As a result of this legislative improvement, the supervisory framework of the SPC had to adapt to the concept of risk-based supervision in order to make an effective verification of the adequacy of an EFPC's internal controls (checking that the requirements or recommendations of Resolution 13 are met). There was, therefore, the need for staff training with a focus on aspects of the governance and control of EFPCs. Another noteworthy development was aligning of the supervisory tools used to the new model. Thus, new software was developed that served as a pilot in conducting supervision, the main goal of which was to analyze the adequacy of EFPC internal controls.

Based on the points indicated by Resolution No. 13 as essential to the management of an EFPC, the software developed provides control points to check the audit of an entity. Its main features are:

- an indication to the auditor of each of the items that must be checked by the supervisor, making a checklist of all the points that the EFPC should fulfil;

[11] The case study was prepared by the Ministério da Previdência e Assistência Social of Brazil

- assigning a specific task to each member of the supervisory staff, matching their knowledge, and making the supervisory process more efficient;

- the centralization of all information collected by supervisors, facilitating processing and analysis;

- sharing and updating information reviewed by auditors with their superiors;

- issuing planning and monitoring reports, work papers, supervisory reports and infraction reports;

- the standardization of supervisory procedures under the Supervisory Department of National Secretariat for Pension Funds.

Despite the advance represented by this tool, the National Secretariat for Pension funds understands that this system is part of a wider project to develop an effective risk based approach to supervision – with all supervisory actions eventually based on this concept.

Finally, the work of the supervisory authority is moving towards creating software that will makes the auditor's work more useful in the analysis of information. It is therefore desirable that this tool is built with the following features:

- centralized access to databases and documents available in the SPC;

- integration into the systems of indicators showing the risk classification of benefit plans;

- processing and information analysis, especially related to investments, accounting and actuarial analysis;

- is incorporated into a supervisory manual;

- be friendly, high reliability and with security requirements.

4. Germany[12]

The German regulatory authority, BaFin, issued a guidance note on '*Minimum Requirements for Risk Management in Insurance Undertakings'* in May 2009, which also applies to pension funds (BaFin 2009). The guidance provides the supervisor with a binding interpretation of the relevant pension law[13] and sets minimum standards for sound administrative procedures and, in particular, appropriate risk management. The guidance is designed to provide a flexible, hands-on framework for risk-management of institutions supervised by BaFin. It is based on the approach that the managers of these institutions must develop a risk awareness, which must be actively supported and kept up at all times.

Within the circular, risk-management includes the definition of an appropriate risk strategy consistent with the chosen business strategy, adequate organisational and operational rules, the establishment of an appropriate internal risk treatment and control system, as well as the establishment of an internal auditing system and the implementation of internal controls. Management is expected to adequately and regularly inform the supervisory body of the risk situation. The guidance outlines minimum requirements, but the supervisory authority reviews and assesses the adequacy of risk management on a proportional basis (i.e. higher standards may need to be applied)[14].

Risk is defined as the possibility of non-achievement of an explicitly formulated or implicitly resultant goal. Risk is considered material if it could have a substantially negative impact on an institution's financial position, performance or cash flows. In order to assess whether or not a risk should be deemed material, management must obtain an overview of the institution's risk profile. The minimum risk categories which should be considered are: underwriting risk; market risk; credit risk; operational risk; liquidity risk; concentration risk; strategic risk; reputational risk. Risk assessment should first be qualitative, with a quantitative assessment undertaken if the risk is deemed material. All managers are responsible for ensuring that the institution has sound administrative procedures.

Institutions must set up a risk-management system with the following essential elements (which should not be considered independently but as dovetailed to from a consistent and interlocking whole, in a holistic approach):

- ***Risk Strategy* –** non-delegable responsibility of the management and to be documented by them. Must address type of risk, risk tolerance, origin of risk, time horizon or risks and the risk-bearing capacity. This should be reviewed at least once a year.

[12] This case study is taken from BaFin's risk-management guidance note (see BaFin 2009)

[13] Since 2008 the 9th amendment of the German Insurance Supervision Act (VAG) (section 64a VAG) introduced the obligation for insurers (including Pensionskassen) and Pensionsfonds to implement an appropriate risk management and to prepare risk and audit reports. With regard to risk management of investment risks, there are special regulations concerning the organisational and operational structure that apply based on other circulars and which remain unaffected by the risk-management circular MaRisk.

[14] The circular notes that risk assessments must take into account the particular features of institutions for occupational retirement provision, and that these, as a rule, are on a limited scale and that their business model is therefore less complex.

- ***Organisational Framework***

  – *Organisational Structure* – should be geared to supporting the most important strategic goals, with a clear separation of incompatible functions (or adequate conflicts of interest arrangements in smaller institutions).

Group within Organisations	**Responsibilities**
Management	• Defining uniform guidelines for risk management, taking internal and external requirements into account • Determining business and risk strategy • Determining risk tolerance and observing risk-bearing capacity • Setting material risk-strategy requirements • Continuous monitoring or the risk profile and establishing an early warning system as well as providing solutions for material risk relevant ad hoc problems
Independent risk control function	• Identification, analysis and evaluation or risks, at least at the aggregate level • Development of methods and processes for risk evaluation and monitoring • Risk reporting on identified and analysed risks and determining risk concentrations • Recommendation of limits • Monitoring limits and risks at aggregate level, monitoring measures to limit risk • Assessing planned strategies under risk aspects • Evaluating new products as well as the current product portfolio in terms of risk • Validating and risk evaluations performed by the business units
Operating Business Units	• Implementing the identification, analysis and, in particular, the treatment of all material risks in their area • Defining and documenting the tasks, responsibilities, representation rules and competencies of the business unit
Internal Audit	• Independently reviewing all business units, processes, procedures and systems following their own procedure and objectively focusing on risk

- *Operational Structure* – should be clearly defined and should support the main functions of the operational structure in line with the risk strategy, enabling all responsibilities and business processes which involve material risks to be determined. Adequate personnel resources are required. New business areas should be integrated. Internal resources and incentive systems should be in line with the risk strategy. IT systems should be suitable and regularly assessed and must ensure the integrity, availability, authenticity and confidentiality of data. The organisational framework, internal risk treatment and controls must be adapted to change s in the environment within an appropriate time period.

- ***Internal Risk Treatment and Control System***

  - *Risk-bearing capacity, concept and limiting* – involving setting up adequate capital requirements

  - *Risk control processes* - risk identification involves recording and classifying all risks, including identifying risk-drivers (internal and external factors which influence risk) and interdependencies. Methods used to identify risk may include structured assessments (i.e. business plan risk assessment), scenario analysis, checklists, standardized questionnaires, trend analysis, expert evaluations/ workshops, interview, Delphi method. The identified risks should then be analysed and evaluated (for probability, correlations), based on meaningful and consistent key figures. Strategies for risk treatment must then be identified (i.e. control metrics identified by business unit), and monitoring systems (undertaken by an independent risk control unit).

  - *Internal Company Communication and Risk Culture* – adequate internal communication of all material risks is necessary. This is the responsibility of the management, but requires and adequate risk culture and awareness of all employees.

  - *Risk Reporting* – this should be clear and concise, and is required regularly to management (depending on level of change), including changes and consequences and impacts of extreme developments.

  - *Quality Assurance, internal risk treatment and control systems* – data, models and procedures should be validated and documented in a transparent way, understandable by third parties.

- ***Internal Audit –*** this should be based on an annual, risk-orientated, comprehensive audit plan. The internal audit function should be objective and independent, with suitably qualified personnel, and full access to information, subject solely to instructions from the management. This function may be outsourced. An overall report should be produced annually, and appropriate assessment to ensure identified deficiencies are rectified should be undertaken.

- ***Internal Controls –*** to ensure the proper functioning of all components of risk management, appropriate control functions should be installed and verified annually, with control weaknesses evaluated and promptly eliminated.

- ***Outsourcing of Functions*** – the risks associated with outsourcing should be identified and evaluated, and outsourced functions should be suitably monitored.

- ***Contingency Planning –*** preparations for crisis situations (when a continuity of business cannot be guaranteed) should be made and regularly reviewed.

- ***Information and Documentation*** – required documentation includes all material formulas, parameters, models, procedures, actions, determinations, decisions, justifications, deficiencies identified and how corrected, as well as changes to risk strategy. All documentation should be comprehensible and verifiable by third-parties.

5. Kenya[15]

Guidance on Risk-Management taking from On-site Inspection Guidelines

Introduction

The objective of undertaking the on-site inspection work is to improve the understanding by the Authority of the level of risks inherent in the particular retirement benefits scheme, focusing in particular on those areas deemed to be significant.

The on-site visit will provide an opportunity to clarify any points arising from the preliminary off-site risk assessment and to gain a better understanding of the operation and management of the retirement benefits scheme.

IT Systems

To assess whether the IT infrastructure, in place, is appropriate to meet the business needs of the retirement benefit scheme under on-site inspection, the Authority shall consider the following:

- Extent to which IT supports the current user requirements or restricts planned initiatives,
- Extent to which IT systems have been assessed in terms of threats to the confidentiality, integrity and availability of key information,
- Adequacy and viability of the IT strategy for the planned initiatives,
- Flexibility to deal with external events

Internal Controls

The objective is to determine the adequacy of the internal control framework and to achieve this, the Authority will assess the decision making framework, the risk management framework, limits and standards, information technology, financial and management reporting, staff policies, segregation of responsibilities, audit and compliance functions.

The sophistication of internal controls will depend on the size of the retirement benefits scheme. The Authority will therefore identify the nature of the activities to be controlled before determining whether the process controls in place are adequate.

Decision making framework

To determine whether the decision making framework is appropriate with delegated authorities and clear accountability at all levels, the Authority will consider; the level of delegation, the adequacy of communication mechanism, means to prohibit individuals without authority from taking decisions or committing the scheme to a transaction, and the adequacy of documentation.

[15] This case study is taken from the Kenya country report prepared for the IOPS Working Paper No.4 (IOPS 2007)

Risk management framework

The Authority will assess the adequacy of systems in place to identify, measure, monitor, and control risk in an appropriate and timely manner. The Authority, in particular, shall focus on the risks associated with the investments and the solvency of the sponsor.

The risks that will be assessed shall include, but are not limited to: operational, credit, interest rate, liquidity, strategic, legal, and information technology. In assessing the risk management framework the Authority will consider; the risk identification responsibility, process and regularity; risk measurement policies; risk monitoring methodologies; risk control measures, and limits and standards

Limit and standards

The Authority will focus on assessing the Board of Trustees and Administrator's risk tolerance and the adequacy of methods used to convey that risk tolerance to the other stakeholders. The Authority will, in particular, assess the experience, background and authority of individuals involved in setting limits; the policy and procedural guidelines; and the processes for setting and changing limits.

Information technology

The Authority will also assess whether controls over the IT infrastructure are appropriate. The Authority will consider the following when assessing the information technology; adequacy of IT resources, prioritization, planning and development; and adequacy of the business continuation plan.

Financial and management reporting

To evaluate the adequacy of the financial and management reporting, the Authority will consider the following:

- Adequacy, accuracy and timeliness of financial and management reporting,
- Ability to assess the quality of assets and maintain an effective level of provisioning,
- Effectiveness and efficiency of distribution, including information sent to Board of Trustees
- Frequency of budget preparation and appropriateness of budgeting process, and
- Explanation of variances

Staff policies

In assessing the various staff policies, the Authority will consider the training initiatives to ensure compliance with the regulations.

Audit and compliance functions

In assessing the audit and compliance functions and procedures, the Authority shall consider the following:

- Responsibility and reporting lines, including their independence,
- Adequacy of processes for addressing exceptions or recommendations on a timely basis,

- Quality and experience of internal audit and compliance management and staff, and
- Links between external audit, internal audit, and compliance

6. Mexico[16]

Internal Risk Management Structure: Requirements for Afores
Operational Risk Committee
Financial Risk Committee
Independent risk units headed by a chief risk officer who reports to the Board
Independent compliance officer (role to be defined by legislation)
Prescriptive regulation that standardizes risk management function across pension funds

Corporate governance of Afores and Siefores is regulated by Consar. Each Afore has to have a board of management of at least five members named by the shareholders, from which at least two must be independent (the proportion of independent members must hold if more than five members are in the board). The independent members must be financial, economic and judicial experts. The board members have specific legal responsibilities. The Board has an important role in managing and controlling operational and investment risks. It is responsible for the constitution of the Operational Risk Committee as well as the Financial Risk Committee for the Siefore, which should propose, respectively, the Operational and Financial Risk Management Policies and Procedures Manuals. The board of management must approve those policies, which are then sent to Consar for endorsement. The board also approves the level of operational and financial risk tolerance of the Afore subject to limits allowed by regulation.

Each Afore is required to have an independent risk unit (*Unidad para la Administración Integral de Riesgos*). This unit is headed by a chief risk officer that reports to the board. The risk unit can be constituted inside the Afore or it may be outsourced (in each case the Afores is responsible for the functions assigned to the unit). This unit supports the Operational and Financial Risk Committees, and it has to identify, measure, monitor and inform the Afore's board of management about the risks faced by the Afore and Siefores, and of any deviation from regulatory limits.

The main functions of the risk unit are: to ensure that the risk management is wide-ranging, suggest methodologies to measure and monitor risks and apply them after they are approved by the risks committees, find out the reasons for deviations of risk limits and detect if these deviations are persistent and inform the risks and investment committees, the board and the independent compliance officer promptly, to supervise the implementation of early warning systems and to ensure timely development and updating of IT systems.

There is also typically an independent compliance officer in each Afore that must have at least 5 years of experience in relevant matters. The role must follow up on observations made by Consar or the external auditor. Because important differences in the role have been observed in different companies Consar is working on new regulation for the compliance officer that would better define what is expected from the role.

The Financial Risk and Operational Risk Committees must comprise one independent member of the board, one non independent member of the board and the person responsible for the independent risk unit.

[16] This case study is taken from the Mexico country report prepared for the World Bank risk-based supervision publication (Brunner et al 2008).

Both committees are directed by the general manager of the Afore. The person in charge of the operational processes in the company and the one involved with financial management as well as the independent compliance officer, must be present in every session of the committee, but do not vote.

For the investment committee, the main tasks are, among others: to define the investment strategies consistent with the investment regime, to define the asset composition of the portfolio, to approve the custodian entity, to approve the reconfiguration of the portfolio in case an investment limit is breached and to define the portfolio benchmark for each fund.

For the risk control committee, the main tasks are, among others: to check the compliance of the investment regime, analyze the risk of the investment strategies, if necessary, contests the prices used for the valuation of the portfolio, to propose the investment strategies to be followed in case of breaching a limit set in the regulation and to judge the portfolio benchmarks in terms of their risk properties.

In addition an independent financial expert is required to evaluate annually the development and functioning of IT systems that are in place to support operations, as well as to supervise that the appropriate modifications to risk models are performed.

In the case of Procesar there has been an important recent change in its corporate governance structure. Previously the owners of Procesar, the Afores and some banks, were each entitled to have one member in the Board of Procesar. However, because of their diverse interests it was not clear that the board was focusing on efficiency especially since the largest member companies were not necessarily supportive of improvements in Procesar that would increase efficiency and reduce barriers to entry and increase competition. To reduce these potential conflicts of interest the structure of the board has been changed, to give greater importance to the independent members of the board. The total number of board members is now set at ten and four of them must be independent, five are represent the Afores and one represents banks. The president of the board has to be one of the independent members.

For the implementation of the RBS approach Procesar is required to have an operational risk committee with similar characteristics to the ones that Afores have.

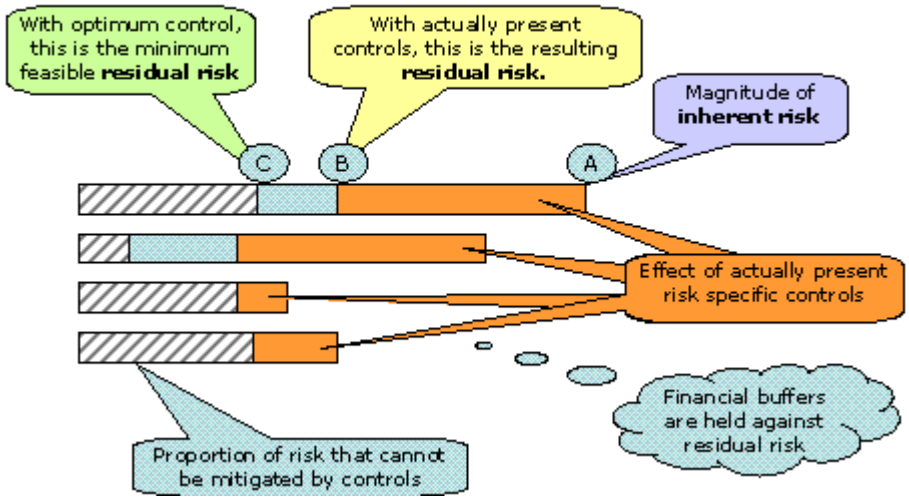
In summary the various committees are the board of management’s arms for managing and controlling risks. They have to approve in a first instance the risk measures and controls proposed by the independent risk unit, and then report to the board. Under the new prudential rules for risk management published in February 2006, the independent risk unit is given the main role in defining methods and procedures for measuring and controlling financial and operational risks. Proposals from this risk unit must be approved by the corresponding committees, which then report to the board of management. Finally, it is a duty of the independent risk unit to inform Consar quarterly about the economic, financial and confidence consequences that the Afore would face if the operational risks materialize.

7. Netherlands[17]

Guidance in FIRM Model

In 2006 the Dutch National Bank (DNB) introduced an integrated method for analyzing risk for all financial institutions known as the Financial Institutions Risk analysis Method (FIRM). Under the FIRM model, the DNB takes into account its assessment of solvency and combines this with an evaluation of the pension entity, the risks to which it is exposed and the quality of the risk management procedures in place. Detailed guidance on the model is provided in the on-line FIRM Manual, including details of how DNB supervisors assess the quality of the risk control systems at the financial institutions which they oversee[18].

The DNB stress that the inherent risks of an institution cannot be reduced to nil, not even with the aid of adequate controls. Phrased differently, even if optimum controls are in place, a residual risk remains in most cases. For some risks, this ultimately resulting residual risk will be larger than for other risks. The supervisor's assessment focuses on the question whether the institution controls the risk concerned in an optimum manner (as best as is realistically feasible). The question whether the risk is thus eliminated in full is of secondary importance. The fact that in many cases risks cannot be controlled completely is reflected in the residual risk calculated by FIRM. Thus, optimum risk-specific control (score 1) for high inherent risks never leads to a residual risk score of 1 within FIRM.



Within FIRM, the following forms of control (control categories) are distinguished[19]:

- risk-specific controls;
- risk-transcending controls (organisation and management);

[17] Case study is drawn from DNB, 'Financial Institutions Risk analysis Method (FIRM) Manual' http://www.dnb.nl/openboek/extern/id/en/all/41-117763.html

[18] http://www.dnb.nl/openboek/extern/id/en/all/41-117836.html - See Annex D.

[19] The FIRM model also considers solvency risk in relation to pension funds –i.e. supervisors consider not only whether solvency requirements have been met but also consider the quality of the solvency management. See the on-line FIRM manual for further details.

- risk-mitigating action of group functions.

Risk-specific Controls	
Control item	***Description***
Risk identification	The degree to which and the manner in which the institution has independently mapped the specific risk category, through such means as a risk inventory and risk analysis.
Risk policy	The quality of the written policy with regard to the degree to which (risk appetite) and the manner in which (outline of controls to be implemented) the institution plans to control the risk category concerned.
AO/IC	The degree to which and the manner in which procedures, function segregations, authorisations, limits and other preventive measures or other measures have been implemented in order to control the risk category concerned and thus to implement the appurtenant risk policy.
Risk monitoring	The degree to which and the manner in which the specific risk is monitored (and required adjustments are made) and the controls have been implemented, for instance by means of performance, incident or exception reports and analyses.

Risk-transcending controls - Organisation	
Control item	***Description***
Organisational structure	The transparency of the legal or organisational structure, and the extent to which it lends itself to promoting effective operations.
Supply of management information	The extent to which timely and reliable financial and operational information is available to responsible staff (including management) permitting them to make timely and well-informed decisions and, where necessary, make timely adjustments.
Human resources	The extent to which adequate HR policies and sound HR instruments are in place, and the qualitative and quantitative adequacy of staff.
Internal cooperation and communication	The extent to which the internal communication and cooperation among departments and business units and with group functions operates, aimed at effective cooperation in the pursuit of the objectives.
Audit measures	The extent to which internal and external audits by auditors and actuaries contribute effectively to the identification, analysis, control, monitoring and reporting of risks.

Risk-transcending Controls – Management	
Control item	***Description***
Management quality and structure	The manner in which the institution's leadership function is effectively performed. Cases in point are: • the competence of the (board of) management as a whole to manage the institution; • the extent to which the (board of) management is adequately balanced in terms of expertise and background; • the extent to which the management structure and composition

	match the size and complexity of the operations; • the extent to which responsibilities have been assigned in an adequate manner to the individual members of the (board of) management and the extent to which an adequate span of control has been realised; • the extent to which the (board of) management sets an example for the institution's staff (for instance, by propagating ethical norms and standards); • the (board of) management's leadership style and the extent to which • the (board of) management is respected within the institution.
Strategy	This concerns: • the manner in which the strategy is formulated within the institution; • the extent to which this process takes place on an institution-wide basis; • the transparency of the process; • the substance and consistency of the strategy; • the degree of specificity of the strategy, and • the extent to which the institution's strategy is clearly and consistently communicated.
Risk/control attitude	This concerns: • the extent to which the (board of) management is aware of and interested in, and has an insight into, the risks to which the institution is exposed; • the preparedness of the (board of) management to use adequate controls (both in-house and underlain by statutory rules) and to make sufficient funds available for that purpose; • the extent to which the (board of) management is prepared to take risks and, when doing so, perform an adequate risk-benefit analysis; • the extent to which the (board of) management complies with the existing internal controls.
Management and decision-making	The extent to which the (board of) management is sufficiently actively and substantively involved in operational management and results. This is reflected in such aspects as the frequency, degree of substantiveness, intensity and action-oriented nature of management consultations. This also concerns the effectiveness of the delegation of powers to (decision-making) bodies (such as risk committees).

Risk-specific controls comprise controls that are specifically aimed at mitigating one single risk category. Thus, collection procedures are aimed specifically at reducing credit risk. Likewise, disaster recovery and back-up procedures are aimed specifically at reducing IT risk. Such risk-specific controls generally seek to reduce the probability of a risk event or, in the case of a risk event, to reduce its impact.

The control category Organisation may exert a risk-mitigating effect on inherent risks through such means as a transparent organisational structure, clear links between activities, management units and group functions, and through an adequate reporting structure. Organisation is a non-risk-specific control, also known as a risk-transcending control. This means that the aspects of Organisation do not relate to a single risk, but have a risk-mitigating effect on the entire functional activity and the risks distinguished in that activity.

The control category Management may exert a risk-mitigating effect on inherent risks through such means as a management structure and composition matching the size and complexity of the operations, an effective decision-making process, effective strategic planning and the encouragement of a corporate culture marked by an awareness of risks and the need for risk control. Like Organisation, Management is a non-risk-specific control, also known as a risk-transcending control. This means that the aspects of Management do not relate to a single risk, but have a risk-mitigating effect on the entire functional activity and the risks distinguished in that activity.

When assessing the controls, use may be made of the assessment criteria where, for each individual risk category, an overview is presented of possible risk-specific controls – which are elaborated in the FIRM manual. For each risk category (interest rate risk, market risk, credit risk, IT risk etc. – 14 in total), the control measures are divided into four categories (risk identification, risk policy, administrative organisation and internal control and risk monitoring). Illustrations of what strong, adequate, inadequate and weak controls would look like are then provided. An example of the sort of controls (across risk categories) which the DNB is looking for is provided in the following table[20].

The controls are scored in the following way:

a) **Strong control**: High control quality makes for a strong reduction of inherent risks. The control framework is fully in line with the requirements set by the nature of the business.

b) **Adequate control**: Adequate control quality makes for an adequate reduction of inherent risks. The control framework is adequately in line with the requirements set by the nature of the business.

c) **Inadequate control**: Control must be improved. Inherent risks are not adequately reduced. The control framework is insufficiently in line with the requirements set by the nature of the business.

d) **Weak control**: Control must be improved drastically and/or immediately. Inherent risks are not or barely reduced. The control framework is barely in line with the requirements set by the nature of the business

e) **Unknown**: If the supervisor has as yet insufficient information about a certain form of control, he/she should use this option.

[20] Details of risk assessment by category are available in Annex D of the FIRM manual.

DNB FIRM Manual Annex D Examples of Strong Risk Controls (across risk categories)
Risk Identification
• Frequent and detailed identification of all relevant aspects of risk category.
• Analysis at least once a year of threats and opportunities posed by the environment (market position, changes in competition, legislative changes and implications etc.).
• Awareness of reputation risk (including contamination from related institutions, customers etc.)
• New products, initiatives and projects are preceded by a thorough analysis of appropriate rate risks. New products may also be approved by a specially appointed approval committee with representatives from management, front-office, risk management and audit.
• Close attention to risks in relation to concentration and correlation in portfolios.
• Risk model has been developed according to best practice methods and is frequently updated, evaluated and independently validated.
• Assumptions and data used in risk modeling are up-to-date, complete, correct, reliable, cover a long horizon and have been drawn from independent sources.
• Management and those concerned at all relevant levels and competencies are involved in risk identification. Full understanding of relevant rate risk among responsible staff.
• Risk identification transparently documented.
• Risk identification based on a systematic approach.
• Risk identification translated into adequate prioritisation.
Risk Policy
• Risk management policy and relevant risk appetite determined by senior management.
• Risk policy is well geared to identify risks that have been designated as important.

• Risk policy indicates extent to which and the manner in which risk should be controlled.
• Policy is of high quality (completeness, level of documentation, quality of content, depth).
• Frequent ALM studies (where appropriate).
• Institution has adopted a comprehensive policy with regard to the use of derivatives.
• Policy has been adequately translated into limits on risks and the maximum impact on the financial position.
• Periodic (reliable) long-term scenario analyses in which a very broad framework of possible disasters/external events is examined.
Administrative Organisation and Internal Control
• Strong embedding in the organisation of the adopted risk policy (as reflected in procedures, segregation of duties, powers, limits and preventive measures).
• Procedures adequately documented and up-to-date
• Tasks, responsibilities and powers are clear and adequate.
• Control takes place in a clear-cut way (a single system) and is centralised in a single group function.
• Adequate segregation of duties and application of four-eye principle with respect to initiation, authorisation, execution, administration and control of investment transactions.
• Full separation between front office and back office.
• Separation between commercial function and market risk management has been implemented up to the highest level in the organisation.
• Clear setting of limits on transactions to be executed and positions to be taken.
• Good limit monitoring, with responsibility for monitoring limits and measurement of exposures has been placed independently from those taking out

these positions.
• Correct, timely and complete recording of transactions performed, risk positions taken and commitments entered into.
• Voice-recording permanently applied in transactions.
• High-quality system for supporting the administration of transactions and positions and for identifying limit overruns.
• Frequent evaluation (back-testing) of assumptions made in sensitivity analyses and stress tests.
• Adequate procedure for independent determination and comparison of prices of both listed and unlisted products.
• Institution makes frequent estimates of outgoing cash flows versus available funds to allow for a timely release of funds.
• Good communication amongst stakeholders.
• Adequate complaints procedure.
• Independent whistleblowers regulation.
• Specification in a service level agreement of highly detailed quality standards.
Risk Monitoring
• Frequent quantification and reporting to top management.
• Frequency of reports is closely geared to the degree of volatility in positions.
• Clear reports.
• Scenario analyses are frequently performed.
• Daily and transparent reports on positions taken, limit overruns and results.

• Very frequent benchmarking of own investment results against the market followed by analysis of deviations.
• Periodic quantitative analysis of concentration and correlation within portfolios.
• Management is periodically informed on status of risks, quality of control and status of improvement measures.
• Apart from reports on the usual risk control activities, frequent standard reports are also submitted on complaints, incidents and exceptions.
• Frequent performance of (reliable) short-term scenario analyses and stress testing in which a very broad framework of possible disasters/external events is examined.

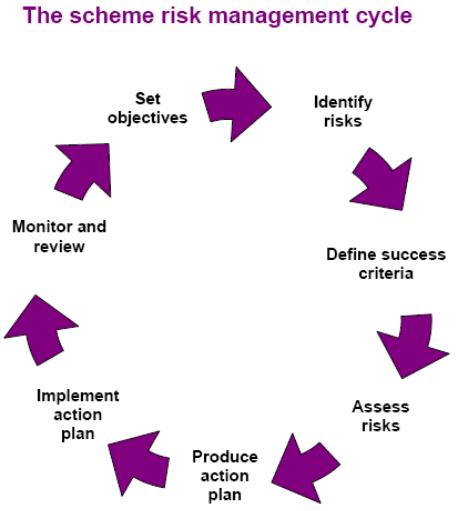
8. UK[21]

The UK Pensions Regulator's Regulatory Code of Practice No. 9 lays out the authority's expectations for how occupational pension schemes should satisfy the legal requirement to have adequate internal controls in place. It is not a prescriptive list for such controls, but rather a high level, risk based approach which trustees may wish to follow when assessing the adequacy of their internal controls. The TRP also stresses that, though all schemes must have internal controls, the trustees must decide on a proportional and suited to the specific nature of their scheme.

Internal controls are defined as:

- arrangements and procedures to be followed in the administration and management of the scheme;
- systems and arrangements or monitoring that administration and management and;
- arrangements and procedures to be followed for the safe custody and security of the assets of the scheme.

The TRP recommends that the trustees identify key risks associated with the functions and activities of the scheme before implementing an internal control framework. The TRP recommend carrying out a risk based review, with the following diagram summarizing one approach to the risk review process and establishing and operating an adequate internal control environment. A non exhaustive list of risks and controls is also provided.



[21] This case study is taken from TPR (2006), 'Regulatory Code of Practice No.9: Internal Controls'
http://www.thepensionsregulator.co.uk/pdf/codeInternalFinal.pd

TPR (2007), 'Codes Related Guidance: Internal Controls'
http://www.thepensionsregulator.co.uk/pdf/InternalControlsGuidance.pdf

Risk	Possible Types of Control (*where appropriate*)
Risk that existing controls are not operating effectively	Periodic control reviews with changes made on a timely basis
Risk of fraud (misappropriation of assets and fraudulent financial reporting)	Segregation of duties; frequent reconciliation procedures for cash and investment balances
Corporate risk (risk of deterioration in strength of employer covenant and ongoing funding)	Monitor financial performance and corporate risk (e.g. inability of employer to fund scheme); procedures in place to detect corporate transactions in the public domain and assess impact on the scheme
Funding/ investment risk (inappropriate investment strategies)	Reconciliation procedures; review of investment strategies; independent peer review of funding advice
Compliance/ regulators risk (failure to comply with scheme rules and legislation)	Compliance audits; stewardship and compliance reports from third parties
Non-compliance or maladministration by administration team or third party advisors e.g. outsourced administrations (poor record keeping)	Peer review of key controls by administration team; authorization procedures; periodic meetings between trustees and provider (when required); service level agreement reviews; performance appraisal of providers; internal quality review procedures by third party administrators (i.e. independent control reviews – 'Assurance Reports')
Computer systems and database failures	System recovery plans; data back-up procedures; password controls
Poor scheme management (ineffective stewardship by those with delegated responsibilities)	Regular trustee meetings; decisions taken within the formal structure of trustee meetings; minutes prepared for all meetings; sub committees; manage conflicts of interest

The TPR also stress that risk assessment is a continuous process and that internal controls should therefore be reviewed periodically (at least annually). However, they also note that any internal controls framework is not infallible and risk cannot be eradicated completely.

As the assessment of risk and internal controls are important features of good governance, TPR suggests that trustees may wish to confirm in their annual report that they have considered the risks facing the scheme and the effectiveness of the controls in place. Third party assessment of the internal controls may also be used.

TRP's related guidance note on complying with internal control obligations – providing more detailed guidance for each step in the risk management process outlined in the diagram above

REFERENCES

APRA (2004), 'Superannuation Guidance NOTE SGN120.2: Risk Management' http://www.apra.gov.au/Superannuation/upload/SGN-120-1-Risk-Management.pdf

BaFin (2009), 'Minimum Requirements for Risk Management in Insurance Undertakings', Circular 3/2009 http://www.bafin.de/cln_152/SharedDocs/Downloads/EN/Service/Rundschreiben/rs___2009__03__marisk__va__english,templateId=raw,property=publicationFile.pdf/rs_%2009_03_marisk_va_english.pdf

Basel Committee on Banking Supervision (2003), 'Sound Practices for the Management and Supervision of Operational Risk' http://www.bis.org/publ/bcbs96.pdf?noframes=1

Basel Committee on Banking Supervision (1998), 'Framework for Internal Control Systems in Banking Organisations' http://www.bis.org/publ/bcbs40.pdf?noframes=1

Basel Committee on Banking Supervision (1997), 'Core Principles for Effective Banking Supervision http://www.bis.org/publ/bcbs30a.pdf?noframes=1

Brunner, G., Hinz, R., Rocha, R., (2008), 'Risk-based Supervision of Pension Funds: Emerging Practices and Challenges'

CEIOPS (2008), 'Implementing Measures on System of Governance' http://www.ceiops.eu/media/docman/public_files/consultations/IssuesPaper-on-Governance.pdf

COSO (1994), 'Internal Control – Integrated Framework' http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990009/PC-990009.jsp

De Nederlandsche Bank, 'Financial Institutions Risk analysis Method (FIRM) Manual' http://www.dnb.nl/openboek/extern/id/en/all/41-117763.html

European Commission (2008), 'Directive of the European Parliament and of the Council on the Taking-up and Pursuit of the Business of Insurance and Reinsurance (Solvency II)' http://ec.europa.eu/internal_market/insurance/docs/solvency/proposal_en.pdf

IAIS (2006), 'A Core Curriculum for Insurance Supervisors'

IAIS (2003), 'Insurance Core Principles and Methodology', http://www.iaisweb.org/__temp/Insurance_core_principles_and_methodology.pdf

IOPS (2008a), 'Guidelines for the Supervisory Assessment of Pension Funds' http://www.iopsweb.org/dataoecd/38/47/41042660.pdf

IOPS (2008b), 'Good Practices in Risk Management of Alternative Investments by Pension Funds' http://www.iopsweb.org/dataoecd/47/20/40010212.pdf

IOPS (2008c), 'Supervisory Oversight of Pension Fund Governance', Working Paper No.8 http://www.iopsweb.org/dataoecd/6/63/41269776.pdf

IOPS (2007), 'Experience and Challenges in Introducing Risk-based Supervision for Pension Funds', Working Paper No. 4 http://www.iopsweb.org/dataoecd/59/27/39210380.pdf

IOPS (2006), 'Principles of Private Pension Supervision' http://www.iopsweb.org/dataoecd/59/7/40329249.pdf

OECD (2009), 'Guidelines for Governance of Pension Funds' http://www.oecd.org/dataoecd/18/52/34799965.pdf

OECD / IOPS (2008), 'Guidelines on the Licensing of Pension Entities http://www.oecd.org/dataoecd/7/34/40434531.pdf

OECD (2006), 'Guidelines of Pension Fund Asset Management' http://www.oecd.org/dataoecd/59/53/36316399.pdf

OECD (2004), 'Recommendation on Core Principles of Occupational Pension Regulation' http://www.oecd.org/dataoecd/14/46/33619987.pdf

The Pension Regulator (2006), 'Regulatory Code of Practice No.9: Internal Controls' http://www.thepensionsregulator.co.uk/pdf/codeInternalFinal.pd

The Pension Regulator (2007), 'Codes Related Guidance: Internal Controls' http://www.thepensionsregulator.co.uk/pdf/InternalControlsGuidance.pdf

World Bank (2007), 'Risk-based Supervision of Pension Funds: A Review of International Experience and Preliminary Assessment of the First Outcomes'

http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2008/01/28/000158349_20080128083737/Rendered/PDF/wps4491.pdf