United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

OFFICE OF INTERNAL OVERSIGHT SERVICES BUREAU DES SERVICES DE CONTRÔLE INTERNE

INTERNAL AUDIT DIVISION DIVISION DE L'AUDIT INTERNE

TO: Mr. Bernard Cochemé, Chief Executive Officer
A: United Nations Joint Staff Pension Fund

Mr. Warren Sach, Representative of the Secretary-General for the investments of the United nations Joint Staff Pension Fund

DATE: 25 Junel 2009

FROM: Ms. Fatoumata Ndiaye, Acting Director
DE: Internal Audit Division, OIOS

REFERENCE: IAD: 09- 02586

SUBJECT: **2009 Comprehensive Risk Assessment – United Nations Joint Staff Pension Fund**
OBJET:

1. This is to inform you that the Internal Audit Division, OIOS has completed the 2009 Comprehensive Risk Assessment of the UNJSPF Secretariat and the Investment Management Service which is provided for your reference.

2. This is the second risk assessment of the Fund. The first risk assessment was conducted with the assistance of Price Waterhouse Coopers in 2005. OIOS was assisted in the current risk assessment by Deloitte & Touche LLP which conducted the focus group interviews and prepared the attached risk assessment register and summary of the risk assessment results.

3. This report of Identified and Summarized Risks is not intended to present a comprehensive representation of all the possible risks that the Pension Fund may encounter. It needs to be updated periodically to reflect changes in the environment, both internal and external, as well as changes in management's perception of risk and risk "appetite." UNJSPF Management may use this information about key risks that came to Internal Audit's attention to support its own risk management activities.

4. A Risk-based Internal Audit Plan for 2009 to 2010 and beyond, which will be aligned with the organization's risk profile, will be formulated with the assistance of the Deloitte team. This plan will be developed in consultation with the Fund and submitted to the Audit Committee for its review on or about 31 July 2009.

5. Please feel free to contact Mr. William Petersen at 212-963-3705 or Mr. Richard Benz at 212-963-5642 if you have any questions.

cc: Mr. Getachew Engida, Chair – UNJSPF Audit Committee
Mr. John Fitzsimon – UNJSPF Audit Committee Member
Ms. Kumiko Matsuura-Mueller – UNJSPF Audit Committee Member
Mr. Carlos Santos – UNJSPF Audit Committee Member
Mr. Tom Repasch – UNJSPF Audit Committee Member
Mr. Mohammad Said – UNJSPF Audit Committee Member
Mr. John McGhie – UNJSPF Audit Committee Member
Mr. Philippe Adhemar – UNJSPF Audit Committee Member
Mr. Jean Lariviere – UNJSPF Audit Committee Member

Deloitte & Touche LLP

100 Kimball Drive
Parsippany, NJ 07054
USA

Tel: 973 602 6000
Fax: 973 602 5050
www.deloitte.com

June 25, 2009

Ms. Fatoumata Ndiaye
Acting Director
Internal Audit Division
Office of Internal Audit Oversight Services
United Nations
2 UN Plaza DC2-518
New York, New York 10017:

Dear Ms. Ndiaye :

Deloitte & Touche LLP ("Deloitte & Touche") has provided certain Internal Audit services on behalf of the United Nations Office of Internal Oversight Services ("OIOS") in accordance with Contract number PD/CO223/08 dated March 5, 2009.

Our work was performed to assist OIOS management in strategizing and planning to conduct a Risk Assessment of the United Nations Joint Staff Pension Fund ("UNJSPF") as well as to assist OIOS in conducting interviews and preparing a risk assessment register and summarizing the results of the risk assessment. Our work was performed during the period March 15 through June 25, 2009 in accordance with the above referenced contract and the applicable International Standards for the Professional Practice of Internal Auditing as prescribed by the Institute of Internal Auditors.

Enclosed is the summarized results of the Risk Assessment excluding the Risk-based Internal Audit Plan, which by mutual agreement will be delivered at a later date. As requested, these results were reviewed in meetings held on May 30, 2009 and June 22, 2009 with management representatives of both the Investment Management Service ("IMS") and Secretariat divisions of the UNJSPF. In addition, OIOS management provided ongoing review and oversight throughout the project. Comments received from management of each of these organizations have been included as deemed appropriate.

This report of Identified and Summarized Risks is intended solely for the information and internal use of the Office of Internal Oversight Services in their development of a Risk-based Plan for Internal Audit and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this report.

Very truly yours,

Deloitte & Touche LLP

Brett Sherman

Brett Sherman, Partner

United Nations Joint Staff Pension Fund

Risk Assessment

Identified and Summarized Risks

June 25, 2009

Section I

PROJECT OVERVIEW AND BACKGROUND

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Risk Assessment Project Overview

The Office of Internal Oversight Services (OIOS) has performed a Risk Assessment of the United Nations Joint Staff Pension Fund (UNJSPF). The purpose of the Risk Assessment was to assist OIOS in prioritizing its Internal Audit activities at UNJSPF for the period 2009 – 2011 and beyond by using a risk-based approach. This approach is considered a leading practice in the Internal Audit profession and is prescribed in the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors (IIA). The Risk Assessment was performed during the period March through June 2009 by Deloitte & Touche LLP professionals under the direction of OIOS.

It is important to emphasize that UNJSPF management has responsibility for monitoring, evaluating and remediating risk within the Pension Fund with oversight from the Audit Committee and in accordance with requirements and directives of the Pension Board. While UNJSPF management is welcome to reference this document, it was not designed for and is not intended to be used as a substitute for management's own continuous risk assessment process including risk evaluation, monitoring, measuring and remediation activities. Further, this assessment, by design, is a subjective assessment. It was not performed in conjunction with auditing procedures, tests of controls or review and analysis of documentation and transactions. Rather, the assessment was based on interviews with UNJSPF personnel supplemented by evaluation of the results of prior Internal Audit activities.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Risk Assessment Project Overview (continued)

The assessment was designed to identify key or significant risks that may or may not be likely to occur as well as to provide an overall framework for recording such risks. It is stressed that the assessments of impact, likelihood and preparedness included in the following details are subjective assessments and that UNJSPF management, with their deeper knowledge and understanding of the Pension Fund's operations, might reach alternative conclusions with respect to specific risks. Further, this Summary and the detailed Risk Register that were developed as part of this project do not make any specific recommendations, as this was not the objective of this assessment and the work performed was not designed to assess the cost benefit or desirability of any alternative procedures, policies or systems to control risk.

It is also important to note that the UNJSPF is highly complex and, as with any Pension Fund, there is substantial inherent risk given the nature of Pension Fund operations, the magnitude of its investments and the millions of individual transactions processed annually. With this in mind, OIOS encourages UNJSPF management to continue its efforts to develop an Enterprise Wide Risk Management (ERM) approach as well as to utilize effective risk management practices in an ongoing and continuous manner to reduce risk to a level that fits within the Organization's risk tolerance.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Current Environment for Pension Plan Sponsors

The current environment for sponsors of large defined benefit pension plans is becoming more challenging.

- Recent economic and capital market uncertainty has had significant negative impact on the funded status of many plans, at a time when plan sponsors' ability to provide additional cash funding to these plans has been strained.
- Increased scrutiny relative to plan management and financial reporting practices has garnered the attention of plan participants and other stakeholders, emphasizing the need for effective processes and sound governance to carry out plan fiduciary duties.
- Although improved management of pension-related risks has become a top priority of many organizations, pension risks are complex, evolving, and require a variety of technical disciplines and expertise (e.g., investment, actuarial) to be effectively managed.

As a result of recent experience, many plan sponsors have a renewed focus on the management of pension risks (financial and non-financial). Plan sponsors are increasingly evaluating various de-risking strategies, including benefit design, investment policy, and liability management, as well as their operating structure.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

UNJSPF Faces Additional Challenges

United Nations Joint Staff Pension Fund ("UNJSPF", "the Pension Fund") has not been immune to the challenges that the current environment has presented. Further, the unique nature of UNJSPF (relative to other large pension funds) presents additional complexities.

- UNJSPF covers over 172,000+ participants and beneficiaries in over 190 countries
- The two-track system is complex (benefits are currently paid in over 15 currencies)
- The administration of UNJSPF is in-sourced, with data management, benefit calculation, contribution collection, benefit processing and payment all handled in-house by personnel in two countries and involving inputs from multiple agencies
- The investment of the majority of UNJSPF pension assets is in-sourced (IMS)
- UNJSPF is subject to the rules and regulations of the UN General Assembly
- Many risks of UNJSPF are interrelated, requiring cooperation across UNJSPF

Given the complexities of UNJSPF and the multitude of risks that exist, it is virtually impossible to manage every risk both simultaneously and optimally. As a result, it is of utmost importance for the organization to identify, quantify, and prioritize its risks - a first step of a cyclical process to maintain an effective risk management program that addresses the areas that are of highest priority and concern to UNJSPF.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Section II

OBJECTIVES, SCOPE AND APPROACH

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Objectives and Scope

Internal Audit's risk assessment project had the following objectives:

- Develop a risk-based plan for OIOS, such that internal audit activities are properly aligned with the organization's risk profile.
- Provide UNJSPF Management with information around key risks that came to Internal Audit's attention

The scope of the risk assessment effort included:

- Performing workshops with the Audit Committee and members of Management and staff across all areas
- Developing a risk register, which is an inventory of key risks and business challenges
- Preparing a risk profile, which prioritizes risks based on impact, likelihood and preparedness
- Proposing an internal audit plan and establishing internal audit priorities

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Overview of Approach

In order to gain an understanding of potential risks that may adversely affect the Pension Fund's ability to achieve its objectives and execute its strategies successfully, 27 workshops were completed and 74 individuals interviewed. The workshops covered the following areas:

- The Secretariat
- Investment Management Services
- Audit Committee

The Pension Fund Risk Map was utilized and updated throughout the project.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Pension Fund Risk Map

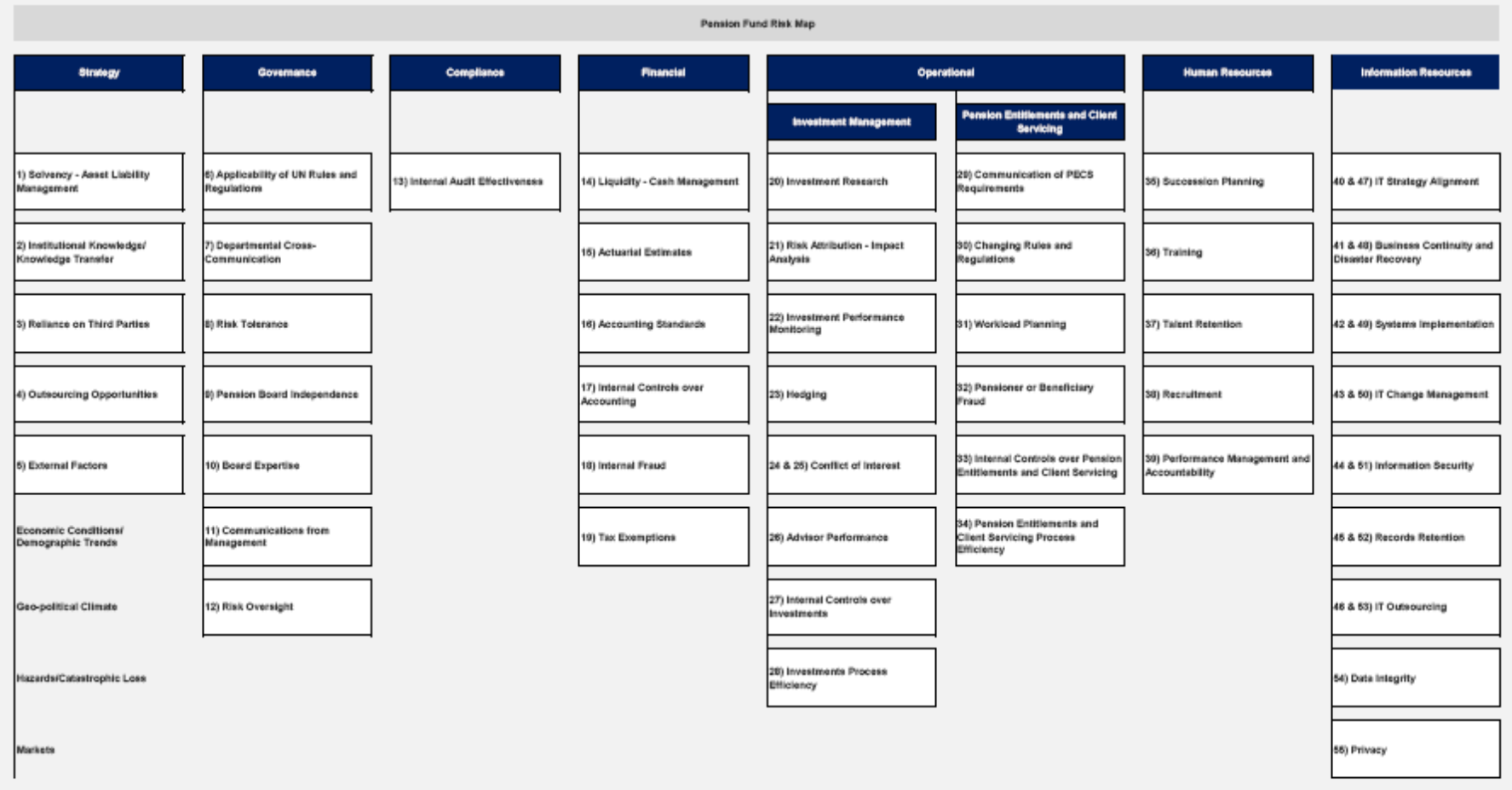
UNJSPF is a diverse and complex international pension system. To better identify the risks that the Pension Fund may face:

- Deloitte's "Risk Intelligence Map" was utilized and customized based on UNJSPF's objectives and strategies
- The customized Pension Fund Risk Map can be used as a tool to:
  - Allow Pension Fund risks to be recognized and categorized as part of management's efforts to assess, prioritize, manage, measure and mitigate risk
  - Demonstrate the inter-connection of risk management silos
  - Identify redundant risk management efforts
  - Improve efficiency in compliance and risk management efforts
  - Develop risk event scenarios that require integrated responses

The Pension Fund Risk Map is not a comprehensive representation of all the possible risks that the Pension Fund may encounter. It needs to be updated periodically to reflect changes in the environment, both internal and external as well as changes in management's perception of risk and risk "appetite."

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Pension Fund Risk Map



This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Section III

SUMMARY OF RESULTS

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Risk Prioritization

For each risk identified on the Pension Fund Risk Map, a description of the risk and Management's assessment of the risk's impact, likelihood and a preparedness rating was documented. Also, an overall risk rating is calculated. These ratings will help to prioritize risks and establish an effective "risk based" internal audit plan.

Impact	**High**	**Medium**	**Low**
Likelihood	**Likely**	**Possible**	**Remote**
Preparedness	**Weak**	**Average**	**Strong**
Overall	**High Priority**	**Moderate Priority**	**Low Priority**

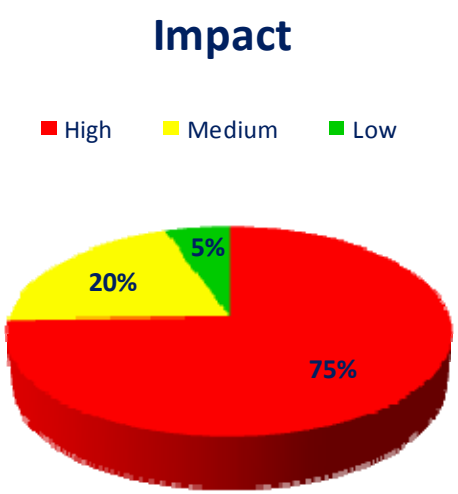
Also, a risk oversight responsibility was identified for each risk among the Pension Board, the Audit Committee and Management.

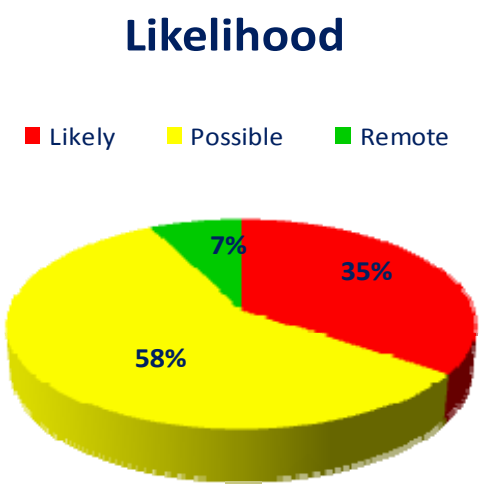
The following slides provide the results of the risk prioritization.

Note: Please refer to Appendix I for Detailed Prioritization Results and Appendix II for rating descriptions

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Summary of Prioritization Results

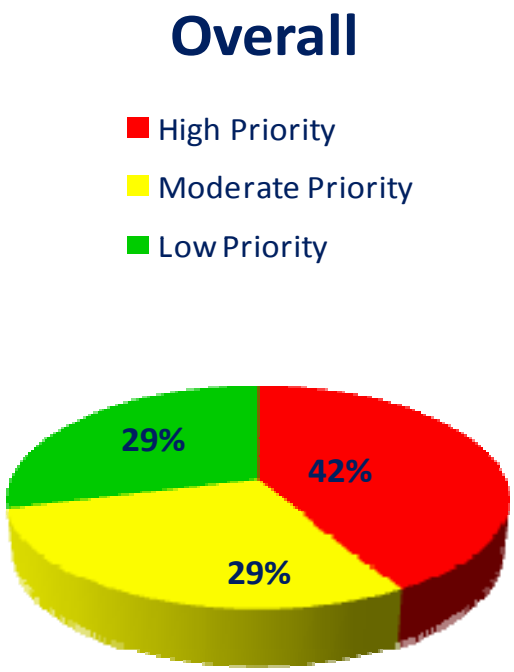




- The Pension Fund faces many high impact risks
- Approximately one third of the risks are more likely to occur
- The Pension Fund is prepared or well-prepared for approximately 60% of the risks with internal controls that meet (or exceed) expected or average requirements.
- For risks that are both high impact and likely to occur, the Pension Fund may wish to consider strengthening overall preparedness.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Summary of Prioritization Results

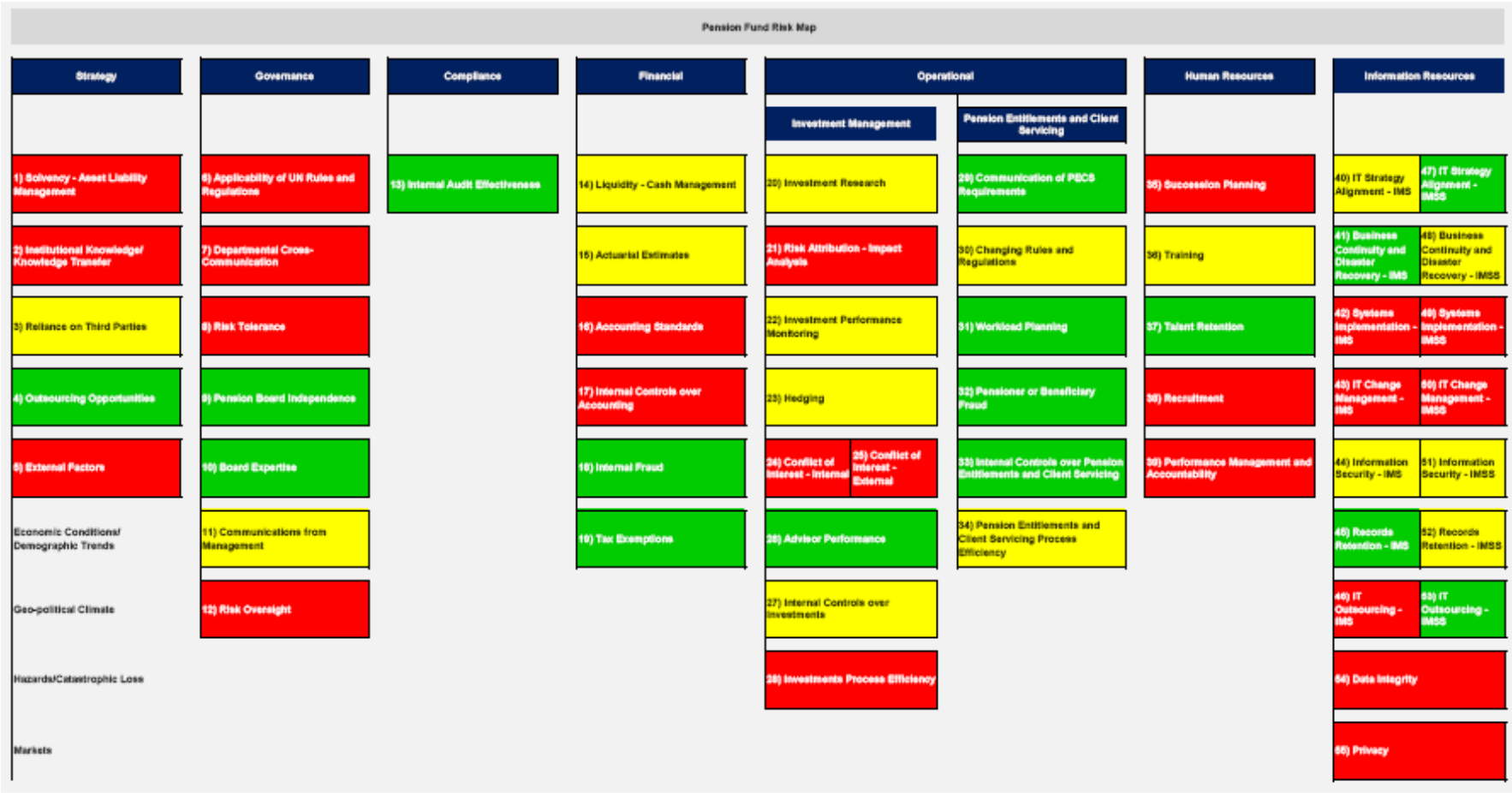


- The overall rating considers the magnitude of impact, the level of preparedness to mitigate the impact and the likelihood of the event happening
- The Pension Fund should give high priority to strengthen mitigation plans for the high priority risks
- The following slides provide detailed description of these high priority areas

Note: Please refer to Appendix II for impact, preparedness and likelihood combinations that result in overall ratings

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Pension Fund Risk Map with Overall Ratings



This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

High Priority Risks

- Solvency - Asset Liability Management
  - The performance of pension plan assets and liabilities are inter-related. Failure to properly manage plan assets and liabilities could result in challenges to honoring present or future pension fund commitments. Asset liability modeling is a tool to assist plan sponsors in assessing their risk tolerance and developing optimal investment strategy as a function of plan liabilities. Proper asset liability management considers:
    - demographic profile of the plan (generational and regional mortality, disability, impact of improved longevity, etc.),
    - capital market volatility and the resulting impact on plan assets and liabilities,
    - macroeconomic elements such as inflation, foreign exchange rates, and interest rate movements.
- Institutional Knowledge/ Knowledge Transfer
  - The complexity of benefit processing, evolution of benefit provisions and increased expectations from participants and pensioners/beneficiaries requires the Pension Fund to document, maintain and allow for effective transfer of the institutional knowledge. The Pension Fund may face operational challenges, unless it documents the institutional memory which resides with its experienced personnel.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

High Priority Risks

- External Factors
  - External factors like political conditions, economic factors, capital markets, social conditions, technological advances, legal and regulatory factors, fraud, and environmental conditions may result in specific risks to the Pension Fund. Occurrence of these factors cannot be controlled by the Pension Fund. While each specific risk cannot be predicted, the fund should be prepared with contingency planning that may not be specific but provides directional guidance (i.e., “what if” scenario analysis). These constant changes and external factors create risk.
- Applicability of Uniform UN Rules and Regulations
  - Some UN rules and regulations were not designed with the Pension Fund in mind, and may have a negative impact on the effectiveness and efficiency of the program's operations.
- Departmental Cross-Communication
  - The pension fund may not effectively address cross-departmental issues or objectives, if the organizational behavior does not support cross-communication. This may result in conflicting goals between the vertical and horizontal structure, insufficient resources, and operational dysfunction. Cross-communication between departments might suffer, resulting in a loss of transparency within the Pension Fund, lack of coordination, and sub-optimal performance of the Pension Fund.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

High Priority Risks

- Risk Tolerance
  - Consistent with the overall objective of achieving optimal results for the Pension Fund, the Pension Board should engage in the appropriate activities to determine the Fund's risk tolerance. The Pension Board and Investment Committee can work closely with senior management to establish and effectively communicate policies that reflect the Pension Board's risk tolerance.
- Risk Oversight
  - The risk-oversight responsibility of management is to ensure appropriate risk-management initiatives are being carried out by the organization. The risk management structure incorporates corporate governance, management review, internal controls, regulatory compliance, and additional assurance as elements necessary for the success of the processes. Consistent with the fiduciary responsibility of the Pension Fund, management should promote a culture of sound risk-management activities, to promote and support the organization in achieving its primary objectives.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

High Priority Risks

- Accounting Standards
  - Failure of the organization to properly apply accounting standards, reporting rules, and regulations in financial reporting may lead to erroneous financial reporting or misstatements. Inability to implement appropriate recognized international accounting standards may result in the incapability to benchmark against other pension funds or leverage a uniform set of accounting standards.
- Internal Controls over Accounting
  - Management presents financial reports to the Board to assist the Board in its decision-making process, and to monitor performance of the organization. The Pension Fund may not have adequate controls in place (such as reconciliations, segregation of duties, and source document verification) to prevent errors or incomplete information from being reported to the Board. Further, should the Pension Fund not examine data reported by internal departments or external parties, this may also result in inaccurate or untimely information being used for decision-making.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

High Priority Risks

- Risk Attribution - Impact Analysis
  - Lack of relevant and reliable tools that enable management to effectively monitor its investment portfolios and attribute performance, as well as understand the sources of risk and how they impact the portfolio's performance, may preclude the Pension Fund from optimizing its risk adjusted performance. Inability of management or Investment Officers to perform attribution analysis may have an impact on individual investments or on the portfolio in aggregate.
- Conflict of Interest
  - Pension funds need an effective process to verify compliance of each investment professional and advisor with rules and regulations around possible conflicts of interest. Non-compliant activities may have a negative impact on the pension fund's reputation. Also, failure to accumulate accurate, relevant and reliable external and internal information to assess compliance may result in the issuance of misleading procedural guidelines and/or decisions.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

High Priority Risks

- Investments Process Efficiency
  - Inefficient processes may be a result of many factors, including outdated technology, expanding operations, and any changes in fund structure. Processes should be continuously monitored to ensure they are optimized and there is no unplanned redundancy. Performance of the Pension Fund can be negatively impacted when it adopts (or fails to improve) inefficient processes and this may have a cascading affect on operations.
- Succession Planning
  - The Pension Fund may fail to use succession planning as a tool to develop and maintain strong leadership and ensure that skills and competencies, built while managing the complex processes of the Pension Fund, are transferred to successors.
- Recruitment
  - The UN's recruiting process may fail to identify a sufficient base of suitable candidates for open positions. The overall process may not address current and future project needs, determine if there are suitable internal candidates to fill positions, move candidates through the process efficiently, and eventually fill open positions with a strong candidate. Also, the process may not utilize all available and appropriate means for identifying candidates.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

High Priority Risks

- Performance Management and Accountability
  - The Pension Fund may not always properly measure and monitor performance and implement incentive programs that motivate and reward its personnel for superior performance. Performance management programs typically include operational performance metrics, behaviors, competencies and adherence to policies. The Pension Fund may fail to implement compensation and incentive programs that reward performing employees appropriately and support retention programs.
- IT Strategy Alignment
  - There is a critical dependence on technology to initiate, record, and manage all aspects of the Pension Fund's transactions and information. Failure to develop, acquire, and implement technologies that are aligned with the Pension Fund's strategies may result in the Pension Fund not fully achieving its objectives.
- Systems Implementation
  - The Pension Fund may encounter difficulty in implementing selected technologies. Implementation issues may include data conversion between different, sometimes incompatible platforms or difficulty in analyzing data. Implementation issues may result in inaccurate calculations, unreliable processing, incomplete recording of data, and disruption of operations.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

High Priority Risks

- IT Change Management
  - Lack of adequate change control procedures, such as access controls, supervisory reviews, approval of change requests, documentation, impact analysis, and segregation of duties (migration from test to production environment by an independent group not involved in programming), may result in unauthorized changes being introduced into the production environment. Implementation of unauthorized, unapproved, or inappropriate changes into a production environment may damage the functionality of the Pension Fund's production systems.
- IT Outsourcing
  - The Pension Fund may contract with an outsourced vendor to perform part or all of the activities typically performed within the Pension Fund's computer processing environments. Typically, such contracts will include a formal service level agreement, which is designed to ensure that the outsourced vendor provides an appropriate level of service to the Pension Fund. Such service level agreements often include, but are not limited to, availability of access to the network, system response times, and turnaround time for problem resolution. The contract often provides a mechanism for measuring performance against the service level agreement and reporting those results to management of the Pension Fund. Failure to monitor the level of service provided and to take appropriate action may result in control deficiencies and/or inefficient or ineffective operations.

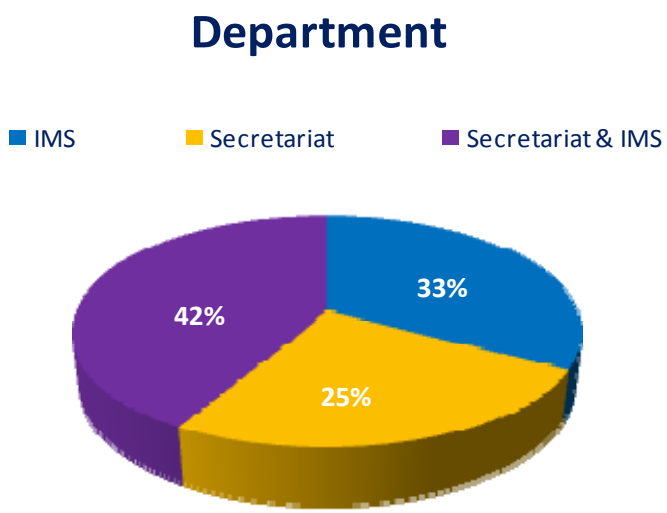
This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

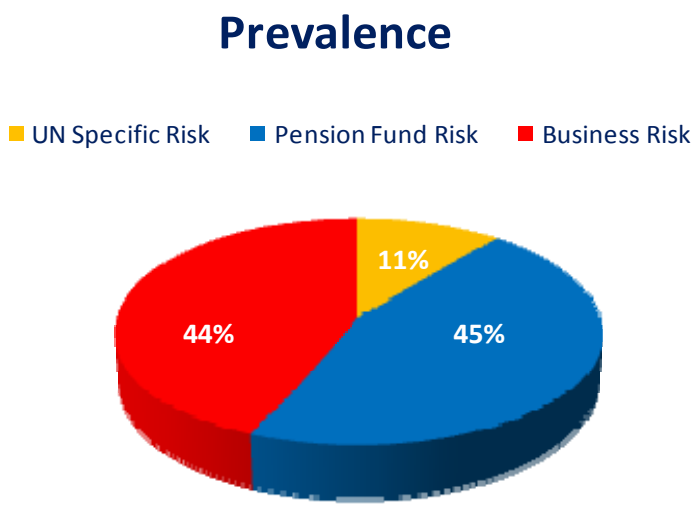
High Priority Risks

- Data Integrity
  - There is a risk if the Pension Fund data is not accurate and complete; or protocols are not in place to assure standardized handling during any use or access (such as transfer, storage or retrieval); and, that data is not protected for its intended use.
- Privacy
  - Unauthorized access to personally identifiable information (PII) creates a significant risk. Dissemination of personally identifiable information can have a negative effect on stakeholders. Protecting PII requires appropriate data classification, which is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of data and documents is essential to differentiate between that which is not sensitive to disclosure and that which is highly sensitive and confidential. The risk exists if data is stored, received, created, or amended without appropriate security and ownership.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Other Information





For each risk, in addition to the risk ratings, other information such as impacted departments and prevalence of the risk among pension funds were also gathered to help Management's risk analysis and mitigation activities

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Appendix I

DETAILED PRIORITIZATION RESULTS

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Detailed Likelihood Prioritization

IMPACT	Remote	Possible	Likely
High	3) Reliance on Third Parties 14) Liquidity - Cash Management 37) Talent Retention 53) IMSS IT Outsourcing	5) External Factors 8) Risk Tolerance 9) Pension Board Independence 10) Board Expertise 11) Communications from Management 15) Actuarial Estimates 16) Accounting Standards 17) Internal Controls over Accounting 20) Investment Research 22) Investment Performance Monitoring 24) Conflict of Interest - Internal 27) Internal Controls over Investments 30) Changing Rules and Regulations 33) Internal Controls over Pension Entitlements and Client Servicing 40) IMS IT Strategy Alignment 43) IMS IT Change Management 47) IMSS IT Strategy Alignment 48) IMSS Business Continuity and Disaster Recovery 49) IMSS Systems Implementation 51) IMSS Information Security 52) IMSS Records Retention 55) Privacy	1) Solvency - Asset Liability Management 2) Institutional Knowledge/ Knowledge Transfer 7) Departmental Cross-Communication 12) Risk Oversight 21) Risk Attribution - Impact Analysis 25) Conflict of Interest - External 28) Investments Process Efficiency 35) Succession Planning 38) Recruitment 39) Performance Management and Accountability 42) IMS Systems Implementation 46) IMS IT Outsourcing 50) IMSS IT Change Management 54) Data Integrity 6) Applicability of UN Rules and Regulations
Medium		4) Outsourcing Opportunities 13) Internal Audit Effectiveness 18) Internal Fraud 23) Hedging 26) Advisor Performance 31) Workload Planning 41) IMS Business Continuity and Disaster Recovery 44) IMS Information Security 45) IMS Records Retention	34) Pension Entitlements and Client Servicing Process Efficiency 36) Training
Low		32) Pensioner or Beneficiary Fraud	19) Tax Exemptions 29) Communication of PECSS Requirements

LIKELIHOOD

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Detailed Preparedness Prioritization

IMPACT	Strong	Average	Weak
High	9) Pension Board Independence 10) Board Expertise 33) Internal Controls over Pension Entitlements and Client Servicing 37) Talent Retention 47) IMSS IT Strategy Alignment 53) IMSS IT Outsourcing	1) Solvency - Asset Liability Management 3) Reliance on Third Parties 11) Communications from Management 12) Risk Oversight 14) Liquidity - Cash Management 15) Actuarial Estimates 20) Investment Research 22) Investment Performance Monitoring 27) Internal Controls over Investments 30) Changing Rules and Regulations 39) Performance Management and Accountability 40) IMS IT Strategy Alignment 48) IMSS Business Continuity and Disaster Recovery 51) IMSS Information Security 52) IMSS Records Retention 6) Applicability of UN Rules and Regulations	2) Institutional Knowledge/ Knowledge Transfer 5) External Factors 7) Departmental Cross-Communication 8) Risk Tolerance 16) Accounting Standards 17) Internal Controls over Accounting 21) Risk Attribution - Impact Analysis 24) Conflict of Interest - Internal 25) Conflict of Interest - External 28) Investments Process Efficiency 35) Succession Planning 38) Recruitment 42) IMS Systems Implementation 43) IMS IT Change Management 46) IMS IT Outsourcing 49) IMSS Systems Implementation 50) IMSS IT Change Management 54) Data Integrity 55) Privacy
Medium		4) Outsourcing Opportunities 13) Internal Audit Effectiveness 18) Internal Fraud 26) Advisor Performance 31) Workload Planning 34) Pension Entitlements and Client Servicing Process Efficiency 36) Training 41) IMS Business Continuity and Disaster Recovery 45) IMS Records Retention	23) Hedging 44) IMS Information Security
Low		19) Tax Exemptions 29) Communication of PECSS Requirements 32) Pensioner or Beneficiary Fraud	

PREPAREDNESS

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Detailed Overall Rating Prioritization

Low Priority	Moderate Priority	High Priority
4) Outsourcing Opportunities 9) Pension Board Independence 10) Board Expertise 13) Internal Audit Effectiveness 18) Internal Fraud 19) Tax Exemptions 26) Advisor Performance 29) Communication of PECSS Requirements 31) Workload Planning 32) Pensioner or Beneficiary Fraud 33) Internal Controls over Pension Entitlements and Client Servicing 37) Talent Retention 41) IMS Business Continuity and Disaster Recovery 45) IMS Records Retention 47) IMSS IT Strategy Alignment 53) IMSS IT Outsourcing	3) Reliance on Third Parties 11) Communications from Management 14) Liquidity - Cash Management 15) Actuarial Estimates 20) Investment Research 22) Investment Performance Monitoring 23) Hedging 27) Internal Controls over Investments 30) Changing Rules and Regulations 34) Pension Entitlements and Client Servicing Process Efficiency 36) Training 40) IMS IT Strategy Alignment 44) IMS Information Security 48) IMSS Business Continuity and Disaster Recovery 51) IMSS Information Security 52) IMSS Records Retention	1) Solvency - Asset Liability Management 2) Institutional Knowledge/ Knowledge Transfer 5) External Factors 6) Applicability of UN Rules and Regulations 7) Departmental Cross-Communication 8) Risk Tolerance 12) Risk Oversight 16) Accounting Standards 17) Internal Controls over Accounting 21) Risk Attribution - Impact Analysis 24) Conflict of Interest - Internal 25) Conflict of Interest - External 28) Investments Process Efficiency 35) Succession Planning 38) Recruitment 39) Performance Management and Accountability 42) IMS Systems Implementation 43) IMS IT Change Management 46) IMS IT Outsourcing 49) IMSS Systems Implementation 50) IMSS IT Change Management 54) Data Integrity 55) Privacy

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Appendix II

RATING DESCRIPTIONS

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Impact Risk Rating Criteria

Criteria	Financial	Reputation (Integrity, Accountability)	Customer	Personnel	Operations	Speed of Onset
High	Significant material financial Impact that may reduce investment gains or negatively impact cash flow	Potential for sustained negative international media attention. Significant loss of reputation. Long recovery period.	Wide-spread impact on customer satisfaction. Serious threat to future growth.	Unplanned loss of several key Personnel. Serious injury to Personnel.	Significant loss of operations. Wide-spread service interruption. Slow system recovery.	Very Rapid – little or no warning, instantaneous.
Medium	Material financial Impact that may reduce investment gains or negatively impact cash flow	Regional media attention that may be sustained. Moderate recovery period.	Decline in customer satisfaction.	Unplanned loss of senior Personnel.	Isolated loss operations. Isolated service interruption.	Several days or weeks.
Low	Immaterial financial Impact that may reduce investment gains or negatively impact cash flow	Minimal local media attention. Quickly contained. Short-term recoverability.	Minimal or isolated impact on customer satisfaction. Minimal complaints and recovery costs.	Unplanned loss of a single associate.	Limited and minimal loss of operations. Promptly recoverable service interruption.	Months or Years.

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Likelihood Risk Rating Criteria - Defined

Criteria	Expectations	Past Experience
Likely	The event is expected to occur in most circumstances	The event has been frequently experienced or is currently being experienced
Possible	The event will probably occur in many circumstances	The event has been experienced before
Remote	The event may occur at some time	The event has not been experienced before

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Preparedness Rating Criteria

Criteria	Control Effectiveness & Efficiency			Capability				Rate of Change
	Controls / Mitigation	Monitoring/ Testing/ Reporting	Audit Findings	People/ Skills/ Knowledge	Third Party	Process	Systems/ Data/ IT/ Security	Expansion or Contraction
Weak	No controls/ mitigation plans exist; Controls/ Mitigation plans exist but are not consistently applied; Controls need to be tested	Ad hoc and informal risk analysis; Risk sources and emerging indicators have not been identified; No formal reporting schedule	Recent audits resulting in high risk findings	Limited level of internal staff capable of managing risk potential; Limited access to external resources	Limited knowledge or influence over vendors and service providers; Costly or limited alternative vendors; High level of dependency on outsourced services	Risk affects a critical process; Risk affects many processes; Risk affects a complex process	Major system performance, reliability and validity issues; Significant security exposures; Outdated and ineffective technology	Significant rate of change experienced by the following resources: business, people, processes, and/or systems
Average	Controls/ mitigation plans need to be updated and improved; Lack of routine controls testing	Risk sources have been identified and are periodically monitored; No formal reporting schedule has been adopted or effectively administered	Recent audits resulting moderate risk findings	Moderate level of internal staff with skill set for managing risk potential; Moderate access to external resources	Moderate influence over vendors and service providers; Alternative vendors are available; Moderate dependency on outsourced services	Risk does not impact a critical process; Risk affects a moderate level of processes; Risk affects only moderately complex processes	Moderate data & system performance, reliability, and validity issues	Moderate level of changes experienced by the following resources: business, people, processes, and/or systems
Strong	Controls/ mitigation plans are in place, consistently applied and routinely tested; Controls/ Mitigation plans are an integral part of standard operations.	Formal risk analysis and reporting schedule embedded in management process; Risk indicators integrated in key processes	Recent audits resulting in low risk findings	Sustainable level of knowledgeable internal staff to manage risk potential; Readily available external resources	Substantial influence over vendors and service providers; Readily available alternative vendors; Isolated dependence on outsourced services	Risk does not impact a critical process; Risk affects a minimal level of processes; Risk affects only simple processes	Minimal data & system performance, reliability and validity issues	Minimal level of changes experienced by the following resources: business people, process, and/or systems

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Overall Rating Criteria

Impact	Preparedness	Likelihood	Overall
High	Weak	Likely	High Priority
		Possible	High Priority
		Remote	Moderate Priority
	Average	Likely	High Priority
		Possible	Moderate Priority
		Remote	Moderate Priority
	Strong	Likely	Moderate Priority
		Possible	Low Priority
		Remote	Low Priority
Medium	Weak	Likely	High Priority
		Possible	Moderate Priority
		Remote	Moderate Priority
	Average	Likely	Moderate Priority
		Possible	Low Priority
		Remote	Low Priority
	Strong	Likely	Low Priority
		Possible	Low Priority
		Remote	Low Priority
Low	Weak	Likely	Moderate Priority
		Possible	Low Priority
		Remote	Low Priority
	Average	Likely	Low Priority
		Possible	Low Priority
		Remote	Low Priority
	Strong	Likely	Low Priority
		Possible	Low Priority
		Remote	Low Priority

This report of identified and summarized risks is intended solely for the information and internal use of the Office of Internal Oversight Services (OIOS) and should not be used by or relied upon by any other person or entity.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Strategic management and governance	Strategy	Secretariat & IMS	**1**	**Solvency - Asset Liability Management**	The performance of pension plan assets and liabilities are inter-related. Failure to properly manage plan assets and liabilities could result in challenges to honoring present or future pension fund commitments. Asset liability modeling is a tool to assist plan sponsors in assessing their risk tolerance and developing optimal investment strategy as a function of plan liabilities. Proper asset liability management considers: - demographic profile of the plan (generational and regional mortality, disability, impact of improved longevity, etc.), - capital market volatility and the resulting impact on plan assets and liabilities, - macroeconomic elements such as inflation, foreign exchange rates, and interest rate movements.	Without proper asset liability management, the Pension Fund may not be able to fulfill its obligations. Therefore, the impact would be **high.** The risk is **likely** because the funded status of the plan may vary significantly based on the prevailing market conditions. There could be a significant asset liability mismatch, meaning that the plan's funded status could be exposed to additional risk under certain economic and capital market environments. Demographic trends are an important consideration. If a new Member Organization joins the plan with significant liabilities in a shorter time horizon, the Pension Fund would have to analyze the impact on the actuarial position of the Pension Fund. **Known control activities and control gaps are as follows:** 1) Currently Member Organization contributions nearly fund the payments. 2) The first ALM study was performed in 2007 by EFI. The ALM was performed when the pension plan was overfunded. 3) The ALM study included some currency risk analysis relating to the two track system; however, feedback indicated that the study could be more robust. IMS is not able to make informed investment decisions relating to currency risk without having full information related to the currency mix of future payments.	High	Likely	Average	High Priority	Strengthen Preparedness	Pension Board	Pension Fund Risk	1. Participants may elect a two track benefit payment. 2. The scope objectives of the asset-liability study that is scheduled for 2006 should be clearly defined.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Strategic management and governance	Strategy	Secretariat	**2**	**Institutional Knowledge/ Knowledge Transfer**	The complexity of benefit processing, evolution of benefit provisions and increased expectations from participants and pensioners/beneficiaries requires the Pension Fund to document, maintain and allow for effective transfer of the institutional knowledge. The Pension Fund may face operational challenges, unless it documents the institutional memory which resides with its experienced personnel.	This risk mainly impacts Pension Entitlements and Client Servicing (PECSS). The impact would be **high** because, without full documentation and effective transfer of institutional knowledge, the Pension Fund may not be able to carry out critical operations in an efficient manner as experienced personnel leave the Pension Fund. This may result in: - inefficiencies and delayed benefit processing - incorrect benefit calculations - over/under payments. The risk is **likely** because: - the Pension Fund faces loss of institutional knowledge through retirement, mobility, death, etc. - it takes seven years to train Senior Benefits Assistants **Known control activities and control gaps are as follows:** 1) PECSS maintains process and case specific documentation; however, documentation is not updated frequently. 2) Changes in rules and regulations affect cases differently; however, case specific application of rules is not clearly documented in all cases. 3) The IPAS system will automate the application of the current rules and regulations on cases, facilitating a streamlined entitlement calculation. It will potentially decrease the need for manual intervention and reliance on experienced personnel. 4) There is a Knowledge Management System (KMS) in place; however, some documents may not be uploaded to KMS. 5) Retention policy for KMS is not clear - all documents in KMS are archived, however, it may be challenging to retrieve specific information. 6) Currently, there is no formal knowledge transfer plan. 7) Exceptions to mobility are granted for occupational groups (Investment Officers and Benefit Officers) which will reduce the likelihood of loss of institutional knowledge with experienced personnel transfers within the UN. 8) It is not possible to promote Senior Benefits Assistants to Benefits Officer, even if they are the best candidates for vacant Benefits Officer positions.	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	UN Specific Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Strategic management and governance	Strategy	Secretariat & IMS	**3**	**Reliance on Third Parties**	Dependency on third party service or product providers creates exposure to default by providers. If the Pension Fund does not periodically perform a formal vendor bidding process, costs or rates may unnecessarily increase. In addition, if the Pension Fund does not diversify its third party providers, this can create additional risks.	The IMS Investments section relies on the following third parties: - Custodian: Northern Trust - Trade Execution: Brokers - Investment Research: Bloomberg, Advisors (both discretionary and non-discretionary) The Operations section relies on the following providers: - Payments: Banks - Actuarial Calculations: Buck Consultants - Information Technology: UNICC If the third party service or product providers listed above became unavailable (e.g. provider goes bankrupt, contract expires) or faces a long-term disruption (e.g. system failure, disaster), the impact on the Pension Fund would be **high,** because it would impact current operations of the plan. Although the Pension Fund depends on single providers as actuarial, custodial and investment research providers, some of these providers historically have been reliable and their long term disruption may be unlikely. Also, there have not been major problems with availability of advisors, brokers and banks. Therefore, the likelihood of the risk is **remote.** **Known control activities and control gaps are as follows:** 1) The Pension Fund is planning to move to a multiple custodian arrangement after Charles River Investment Management System (Charles River) implementation. The Pension Fund will assess the sufficiency of the insurance coverage with the custodians. 2) The Pension Fund does not have written contracts with brokers. 3) Bloomberg is the major investment research provider. The procurement process has delayed the renewal of the Bloomberg contract. 4) The Pension Fund periodically evaluates performance of its advisors using an evaluation form. 5) The Pension Fund has contracts in place with the banks. There are some cases when only one bank is used for a specific payment type. For example, for payroll payments in Geneva, UBS is primarily used; therefore, UBS's availability is crucial for the Pension Fund to continue its payroll payments. 6) The Pension Fund has been using Buck Consultants since 1949. Buck Consultants maintain significant institutional knowledge given their experience with the plan over this time period. 7) The existing procurement process has a negative impact on contract renewals, given the time it takes to secure a contract.8) Current economic environment lends to probability of mergers, acquisitions and bankruptcy among vendors.	High	Remote	Average	Moderate Priority	Strengthen Preparedness	Management	Business Risk	1. Actuarial assumptions/cost analysis 2. Banking Relationships 3. Procurement of contractual services. 4. The move to a single MRK and custodian will require some process changes.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Strategic management and governance	Strategy	Secretariat & IMS	**4**	**Outsourcing Opportunities**	The Pension Fund must be aware of its business needs and changing environments. The benefits of outsourcing range from risk mitigation to decreased costs. The Pension Fund may not realize the opportunity to use the core competencies of other organizations to gain efficiencies. In addition, the Pension Fund may miss the opportunity to focus on improving its own strengths.	As the Pension Fund currently uses mostly internal resources for carrying out its operations (including investment management), it may not benefit from certain outsourcing opportunities; this may result in inability to reduce costs or benefit from expert advice. The impact would be **medium.** The risk is **possible,** because there are opportunities to outsource certain areas under client servicing, benefits processing, and investment management operations. **Known control activities and control gaps are as follows:** 1) The Pension Fund uses internal resources for benefits processing and client servicing. 2) The Pension Fund uses discretionary advisors for a portion of its investments. Other investment management activities are carried out by internal Investment Officers.	Medium	Possible	Average	Low Priority	Verify Preparedness	Management	Pension Fund Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Strategic management and governance	Strategy	Secretariat & IMS	**5**	**External Factors**	External factors like political conditions, economic factors, capital markets, social conditions, technological advances, legal and regulatory factors, fraud, and environmental conditions may result in specific risks to the Pension Fund. Occurrence of these factors cannot be controlled by the Pension Fund. While each specific risk cannot be predicted, the fund should be prepared with contingency planning that may not be specific but provides directional guidance (i.e., "what if" scenario analysis). These constant changes and external factors create risk.	The following are examples of external factors that may have a **high** impact on the Pension Fund's operations: 1) Economic Conditions/Demographic Trends (Primarily Affect: IMS/PECSS; Impact Overall Solvency of the Pension Fund) a) Macroeconomic factors b) Demographic factors c) Inflation/deflation d) Monetary and Fiscal Policies 2) Geo-political Climate (Primarily Affect: PECSS) a) Political Instability b) Corruption c) Cultural Disconnect 3) Hazards/Catastrophic Loss a) Health Epidemics b) Natural Disasters c) Terrorist Attacks 4) Markets (Primarily Affect: IMS; Impact Overall Solvency of the Pension Fund) a) Capital Markets b) Commodity Markets c) Interest Rates d) Foreign Exchange Rates All of the above present risks and are **possible.** **Known control activities and control gaps are as follows:** 1) The Pension Fund plans for certain risks it can control; however, it follows a reactionary approach to other external factors. 2) The Pension Fund is developing a Global Risk Management Plan. 3) The Pension Fund needs to update the IMS infrastructure and improve risk management process to better manage market risk	High	Possible	Weak	High Priority	Strengthen Preparedness	Management	Pension Fund Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Strategic management and governance	Governance	Secretariat & IMS	**6**	**Applicability of UN Rules and Regulations**	Some UN rules and regulations were not designed with the Pension Fund in mind, and may have a negative impact on the effectiveness and efficiency of the program's operations.	Due to inflexibility and the nature of the UN rules and regulations applicable to the Pension Fund (e.g. procurement, recruitment, mobility, etc.), the Pension Fund may face inefficiencies while: - working towards achieving program goals - addressing new issues - taking advantage of emerging opportunities (e.g. new investment products). This has a **high** impact on its operations. The Pension Fund's objectives include fiduciary aspects as well as an investment management aspect, whereas other UN programs have solely non-profit objectives. The Pension Fund currently faces inefficiencies because of the uniform UN rules and regulations. Therefore, the risk is **likely.** **Known control activities and control gaps are as follows:** 1) It may take up to a year to update a policy. This timeline may fail to support the Pension Fund's business which is more dynamic in nature (e.g. new investment products) 2) IMS is unable to implement tools due to procurement related issues (e.g. inability to implement Credit Suisse's HOLT tool because of soft dollar restrictions). 3) Budgetary process is performed two years in advance and approved by the Pension Board. The budget is not updated frequently to adapt to the changing environment on a more dynamic basis. 4) Rules are unclear to employees/staff and this can cause duplicate efforts in trying to process simple requests. 5) The Pension Fund has a limited Delegation of Authority (DOA) for Procurement & HR.	High	Likely	Average	High Priority	Strengthen Preparedness	Pension Board	UN Specific Risk	1. Procurement policies established by the UN and/or UN's legal status may hinder timely access to necessary tools.
Strategic management and governance	Governance	Secretariat & IMS	**7**	**Departmental Cross-Communication**	The pension fund may not effectively address cross-departmental issues or objectives, if the organizational behavior does not support cross-communication. This may result in conflicting goals between the vertical and horizontal structure, insufficient resources, and operational dysfunction. Cross-communication between departments might suffer, resulting in a loss of transparency within the Pension Fund, lack of coordination, and sub-optimal performance of the Pension Fund.	The impact of this risk is **high** because without effective cross-communication the Pension Fund may fail to effectively address cross-departmental issues or objectives and duplicate administrative efforts. Currently, the CEO is responsible to the Board while the director of the IMS reports through the RSG to the SG. Therefore, the risk is **likely.** **Known control activities and control gaps are as follows:** 1) There are certain programs in place to improve the communication between these two divisions (e.g. working groups) 2) Office of the CEO and IMS are in the process of drafting a Memorandum of Understanding (MoU). 3) A MoU has been signed for the IMSS IT services & IMS IT Services.	High	Likely	Weak	High Priority	Strengthen Preparedness	Pension Board	UN Specific Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Strategic management and governance	Governance	IMS	**8**	**Risk Tolerance**	Consistent with the overall objective of achieving optimal results for the Pension Fund, the Pension Board should engage in the appropriate activities to determine the Fund's risk tolerance. The Pension Board and Investment Committee can work closely with senior management to establish and effectively communicate policies that reflect the Pension Board's risk tolerance.	IMS Investments and IMS Risk Management sections are responsible for implementing investment policy with the risk tolerance established by the Pension Board. The impact of a sub-optimal process to determine risk tolerance level would be **high** because: - a high risk tolerance could result in high asset losses - a low risk tolerance may result in lost income or asset enhancement opportunities. Determining the appropriate risk appetite and tolerance depends on the Pension Board's expertise in the pension investments area (or reliance on third parties that have pension investment expertise), as well as cross coordination between relevant parties. As Pension Board members or third parties with advisory capacity changes, likelihood changes; therefore, the risk is **possible.** **Known control activities and control gaps are as follows:** 1) The Investment Policy defines the risk tolerance levels. Investment Policy also outlines the strategic asset allocation based on the risk tolerance (e.g. the Investment Committee authorized use of certain derivatives). It is reviewed and approved by the Pension Board. 2) Investment Committee performs an advisory role in developing the risk tolerance. 3) Strategic asset allocation is the most important factor in long term performance. A risk attribution tool is required to monitor the strategic asset allocation set forth in the Investment Policy. Currently, this tool is not in place. Investment Officers meet weekly to engage in active oversight of fund performance. 4) Without an effective risk attribution tool, it is difficult to appropriately assess the risk of the portfolio.	High	Possible	Weak	High Priority	Strengthen Preparedness	Pension Board	Pension Fund Risk	1. Asset allocation, benchmark selection and investment mandates may result in suboptimal returns. 2. Alternative Investments can provide higher returns with greater risk, but are not an approved asset class. 3. Securities lending is currently not an approved activity.
Strategic management and governance	Governance	Secretariat & IMS	**9**	**Pension Board Independence**	Lack of an appropriate level of independence represented by a sufficient number of members may result in the failure of the Pension Board and other governance bodies to provide sound advice, counsel, and direction, and to serve as a necessary check and balance on management. Furthermore, an appropriate composition is required to provide diverse perspectives, country specific insights, and expertise in areas needed by the respective member organizations.	Impact would be **high** because, without independence (or a perception thereof), decisions might be made that would impair the Pension Fund's reputation. The Pension Fund should be able to demonstrate that it serves all countries and member organizations equally. The Pension Fund serves 23 member organizations and invests internationally, therefore the risk is **possible.** **Known control activities and control gaps are as follows:** 1) The Pension Board is tripartite in nature and composed of: 1/3 representatives of member organizations, 1/3 governing bodies, 1/3 executive heads. 2) Changes to the regulations are made by recommendations proposed by the SPCs, Member Organizations, countries, participants and stakeholders. Changes are approved by the Pension Board and by the General Assembly. 3) Pension Board recommendations to the rules and regulations needs to apply to all member organizations. 4) The Pension Board may make recommendations against the regulations of the Pension Fund. There may be a need for the legal counsel to advise the Pension Board. 5) The Pension Board receives analytics regarding projected costs associated with recommended changes to the rules and regulations.	High	Possible	Strong	Low Priority	Verify Preparedness	Pension Board	Pension Fund Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Strategic management and governance	Governance	Secretariat & IMS	**10**	**Board Expertise**	Failure on the part of the governance bodies to stay abreast of relevant financial, operational, governance, and regulatory developments as it relates to the Pension Fund may result in inappropriate or sub-optimal decisions, exposing the Pension Fund to excessive risk. The Pension Fund should ensure that the governance bodies receive necessary information to foster an effective decision making process.	Without adequate expertise and ability to stay abreast of developments in the pension industry, the Pension Board, the Audit Committee and senior management may not be able to make the most effective decisions and the Investment Committee and the Committee of Actuaries may not be able to provide effective advice. The impact would be **high.** As members of these governance bodies change, the likelihood changes. Therefore the risk is **possible.** **Known control activities and control gaps are as follows:** 1) The Pension Board may make recommendations against the regulations of the Pension Fund. There may be a need for the legal counsel to advise the Pension Board. 2) Secretariat & IMS implemented a training program for new Board Members. 3) The Pension Board directs the Secretariat to hire consultants/experts to perform certain studies.	High	Possible	Strong	Low Priority	Verify Preparedness	Pension Board	Pension Fund Risk	New
Strategic management and governance	Governance	Secretariat & IMS	**11**	**Communications from Management**	Governance bodies need timely access to accurate and complete information to make informed decisions. Hence, management should help foster an environment that is conducive to open and direct communication. Failure of management to communicate critical information to the governance bodies in a timely manner may hamper collaborative and effective decision-making.	Without adequate information, the Pension Board and the Audit Committee may not be able to make the most effective decisions and the Investment Committee and the Committee of Actuaries may not be able to provide effective advice. The impact would be **high.** As senior management changes, likelihood changes. Therefore the risk **possible.** **Known control activities and control gaps are as follows:** 1) On occasion, the Audit Committee has faced challenges in receiving complete information as it relates to details of financial reporting, despite posing follow up questions to appropriate personnel.	High	Possible	Average	Moderate Priority	Strengthen Preparedness	Management	Pension Fund Risk	New
Strategic management and governance	Governance	Secretariat & IMS	**12**	**Risk Oversight**	The risk-oversight responsibility of management is to ensure appropriate risk-management initiatives are being carried out by the organization. The risk management structure incorporates corporate governance, management review, internal controls, regulatory compliance, and additional assurance as elements necessary for the success of the processes. Consistent with the fiduciary responsibility of the Pension Fund, management should promote a culture of sound risk-management activities, to promote and support the organization in achieving its primary objectives.	A risk management structure is required for overall operations of the Pension Fund. Without an effective risk management process, the Pension Fund may not identify, prioritize, and mitigate potential risks. The impact would be **high.** Currently, the Pension Fund has a Risk Management function under IMS, focusing on investment risks. However, there is no formal risk management function that oversees corporate governance, management review, internal controls, compliance, and additional assurance as elements. Therefore, the risk is **likely.** **Known control activities and control gaps are as follows:** 1) The Pension Fund has issued an Enterprise-wide Risk Management Policy in April 2006 with the help of an outside provider, PWC. The Risk Management Policy has not been updated since then. 2) Management prepared a SWOT analysis in October 2007. 3) There is a proposal to create a Risk Management Unit within the Secretariat, and there is a Risk Management Unit within IMS, however; there is not a consolidated risk oversight function. 4) There is a risk management function within IMS. This enables IMS to have an explicit function that is responsible and accountable for identifying the various risks associated with its business, and to provide input on strategies and tools to better mitigate and manage risk. To date, however, certain personnel within the risk management function have been primarily focused on management reporting.	High	Likely	Average	High Priority	Strengthen Preparedness	Audit Committee	Business Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Compliance	Secretariat & IMS	**13**	**Internal Audit Effectiveness**	Internal Audit planning is required to determine the timing, nature and extent of audit procedures to be performed on operational, financial and compliance areas. Such procedures should be designed to detect errors that are material to the organization's operations or reports. Internal Audit resources must be appropriately allocated for process innovation and internal control improvements to ensure compliance in a more effective and efficient manner.	Without a risk based approach and expertise in the Pension Fund's operations, Internal Audit may not be able to provide value add services. Cost of internal audit, time commitment by management and ineffective internal audit recommendations may have an impact on operations. The impact would be **medium.** The risk is **possible** because IMS expressed reservations to the Audit Committee about the internal audit activities. **Known control activities and control gaps are as follows:** 1) Internal Audit employs a risk based approach 2) Internal Audit uses expert consultant for specific projects 3) All OIOS dedicated professional staff are certified	Medium	Possible	Average	Low Priority	Verify Preparedness	Audit Committee	Business Risk	New
Financial management	Financial	Secretariat & IMS	**14**	**Liquidity - Cash Management**	Ineffective management of liquidity can result in difficulty in meeting pension fund obligations (specifically, benefit payments). Liquidity risk is failure of the pension fund to meet financial obligations as they become due because of an inability to liquidate assets or obtain adequate funding, or the inability to easily unwind or offset specific exposures without significantly lowering market prices because of inadequate market depth or market disruptions ("market liquidity risk"). Liquidity risk may result in the organization having insufficient resources to maintain operations without interruption.	Without appropriate liquidity management, the Pension Fund may run into challenging issues, such as being forced to liquidate certain assets at inopportune times. Impact would be **high.** The risk is **remote** because: - currently 3-5 % of the Pension Fund's assets are in cash, - the majority of other investments are fairly liquid, and - currently, monthly contributions are greater than benefit payments, providing additional liquidity. **Known control activities and control gaps are as follows:** 1) A daily cash report is used for reconciling currencies, dividends and interest between IMS' records and the custodian's records that allows the Cash Desk to project the cash position of the Pension Fund. 2) Investment Officers have executed trades based on unknown cash position (e.g. anticipated cash dividends, foreign currency availability) resulting in overdraws. 3) BOA and OIOS have performed various audits and audit recommendations are either implemented or in the process of being implemented.	High	Remote	Average	Moderate Priority	Strengthen Preparedness	Management	Pension Fund Risk	1. Banking Relationships 2. Funding of Pension Payment Account

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Financial management	Financial	Secretariat & IMS	**15**	**Actuarial Estimates**	Pension liabilities are subject to periodic actuarial estimation. Actuarial estimates may be inaccurate for a number of reasons, including but not limited to: compromised census data quality, inappropriate assumptions regarding future demographic experience, and incorrect methods of calculation.	Without appropriate use of actuarial estimates, the Pension Fund may not have visibility into its funded position and may not be able to sustain payments. The impact is **high.** The consulting actuary, Buck Consultants, is experienced in the Pension Fund's operations; however, it relies on the integrity of the data provided by the Pension Fund. There is a possibility that the data may not be completely accurate. Also, the changing environment and regional differences complicates demographic assumptions that have direct impact on the Pension Fund's liabilities. Therefore, the risk is **possible.** **Known control activities and control gaps are as follows:** 1) Buck Consultants has been the actuary for the Pension Fund since 1949 2) Pension data integrity (both active and inactive participants) is dependent on the accuracy of data received from the Member Organizations 3) Current payroll is used as a base for future payments; however, the two-track system allows participants to choose different currencies for future payroll, greatly complicating liability estimates.	High	Possible	Average	Moderate Priority	Strengthen Preparedness	Management	Pension Fund Risk	1. Participants may elect a two track benefit payment.
Financial management	Financial	Secretariat & IMS	**16**	**Accounting Standards**	Failure of the organization to properly apply accounting standards, reporting rules, and regulations in financial reporting may lead to erroneous financial reporting or misstatements. Inability to implement appropriate recognized international accounting standards may result in the incapability to benchmark against other pension funds or leverage a uniform set of accounting standards.	Without utilization of appropriate pension accounting standards, the Pension Fund may not be able to properly analyze its financial status on an accounting basis. The impact would be **high.** The risk is **possible** because the Pension Fund is in the process of adopting and internationally accepted financial reporting framework. **Known control activities and control gaps are as follows:** 1) UN is using UNSAS standards. The Pension Fund has a plan to adopt certain aspects of IPSAS and IFRS, which has specific standards for Pension Funds. 2) Currently, the Pension Fund is reporting assets based on cost and reporting the market value of assets in disclosures. This may create a risk of overstating assets.	High	Possible	Weak	High Priority	Strengthen Preparedness	Management	Business Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Financial management	Financial	Secretariat & IMS	**17**	**Internal Controls over Accounting**	Management presents financial reports to the Board to assist the Board in its decision-making process, and to monitor performance of the organization. The Pension Fund may not have adequate controls in place (such as reconciliations, segregation of duties, and source document verification) to prevent errors or incomplete information from being reported to the Board. Further, should the Pension Fund not examine data reported by internal departments or external parties, this may also result in inaccurate or untimely information being used for decision-making.	Without sufficient information systems and competent staff, the Pension Fund may not be able to generate reliable financial information, which would have a **high** impact on the Board's decisions. The risk is **possible** because certain information on the financial statements is generated by third parties or by departments that are independent from each other. **Known control activities and control gaps are as follows:** 1) Certain staff turnover has occurred and may occur in the future (information technology personnel presented as a specific known risk). 2) Master Record Keeper records should be reconciled against the Custodian records; this is currently performed by the same provider (Northern Trust). The new custodian RFP requires independent record keeper. 3) Responsibilities are not clearly delineated between IMS & Financial Accounting; account and trading reconciliations are performed, but reconciling items may go uncorrected. 4) IT team created reports to reconcile Abacus (IMS Accounting Software) to the custodian records on a daily basis. 5) On at least one occasion, details of certain budget items could not be provided in a timely manner to the Pension Board.	High	Possible	Weak	High Priority	Strengthen Preparedness	Management	Pension Fund Risk	1. The accounting for real estate transactions is cumbersome and results in unreliable estimates. 2. The current close process takes four months.
Financial management	Financial	Secretariat & IMS	**18**	**Internal Fraud**	Segregation of duties is a key concept of internal control. It is based on the premise that no single individual has control over conflicting phases of a transaction or operation. Deliberate fraud is more difficult because it requires collusion of two or more individuals or parties. The Pension Fund needs to ensure that information systems and user departments are organized in a way to achieve adequate segregation of duties. Failure of the Pension Fund to implement adequate segregation of duties may lead to perpetration of internal fraud.	The Pension Fund may face fraud related to selection and use of service providers, procurement, and benefit payments to illegitimate pensioners/beneficiaries. The impact would be **medium** because although fraud would likely be perpetrated on case by case basis, there would be a reputational impact. The risk is **possible** although segregation of duties appears to have been properly established in the organizational structure. **Known control activities and control gaps are as follows:** 1) Entitlements process duties are segregated organizationally. Document receipts, benefit calculations, audits, benefit releases, and certification are performed by different staff. 2) Payment process activities that a user can perform are segregated by roles established in the Lawson system. 3) Benefits are only paid if the Member Organization makes contributions for the participant. Therefore, the risk of fictitious participants is low. 4) Controls to monitor and detect fraudulent cases may not be strong.	Medium	Possible	Average	Low Priority	Verify Preparedness	Management	Pension Fund Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Financial management	Financial	IMS	**19**	**Tax Exemptions**	Lack of complete understanding of tax provisions and improper planning of a pension fund's operations can result in loss of tax exemptions and deductions.	The risk relates to lost tax exemption opportunities (rather than a direct impact on the value of investments and potential future liabilities). The lost opportunity is only relevant to those countries that allow tax exemptions. Therefore, the impact would be **low.** The risk is **likely** because all countries are supposed to provide tax exemptions; however, often they are not actively enforced, requiring significant efforts by UN personnel to recover these tax benefits. The Pension Fund needs monitor and identify opportunities. **Known control activities and control gaps are as follows:** 1) All investments are evaluated to ensure a favorable tax outcome. 2) Tax exemption rules may place a limit on tax benefits for certain types (or geographical location) of investments. The structure of an investment is determined based on tax exemption rules. 3) Tax implications of small cap investments may not be effectively monitored (since small cap investment management is outsourced). 4) Office of legal counsel needs to assert the Pension Fund's rights with the countries. 5) Follow up with custodian bank is required to claim this income.	Low	Likely	Average	Low Priority	Re-evaluate Impact of Combined Risks	Management	Pension Fund Risk	1. Tax Compliance Issues
Program and project management	Operational	IMS	**20**	**Investment Research**	The Pension Fund invests in a variety of asset classes and investment vehicles. As a result, it may face market risk, credit risk, interest rate risk, currency risk, and liquidity risk. Lack of appropriate research to enhance knowledge of different markets, economic factors, political and regulatory changes, monetary policies, global trends, capital markets, security specific factors, or inadequate risk analysis may result in sub-optimal investment performance or fiduciary risks.	Poor investment decisions may result in loss of assets. The impact would be **high.** The risk is **possible** because: - Investment Officers are restricted to limited tools for internal research, and - Advisors may provide inaccurate or poor quality information. **Known control activities and control gaps are as follows:** 1) The Pension Fund uses a bottom-up research process. 2) Equity and Fixed Income groups use the following: a) Investment research tools (i.e. Bloomberg) b) Experienced Investment Officers c) External advisors Investment Advisors uniformly approve the suggested investments. The use of Investment Advisors delays the transaction, potentially impacting returns. The Investment Officers make the final investment decisions and are measured on the performance of those decisions. IMS tracks the quality of external advisors' recommendations. 3) Alternative Investments and Real Estate perform the following: a) Up front due diligence for closed-end investments b) Legal & regulatory research for long term investments 4) There is no dedicated research function. 5) Investment tools are not uniformly available to all investment groups due to licensing restrictions (e.g. Thompson). 6) Risk and Compliance function performs reviews	High	Possible	Average	Moderate Priority	Strengthen Preparedness	Management	Pension Fund Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Operational	IMS	**21**	**Risk Attribution - Impact Analysis**	Lack of relevant and reliable tools that enable management to effectively monitor its investment portfolios and attribute performance, as well as understand the sources of risk and how they impact the portfolio's performance, may preclude the Pension Fund from optimizing its risk adjusted performance. Inability of management or Investment Officers to perform attribution analysis may have an impact on individual investments or on the portfolio in aggregate.	Without proper attribution analysis, portfolio risk may not be effectively monitored and managed, resulting in undesirable results. Therefore, impact would be **high.** Currently, IMS does not have a tool to perform attribution analysis for certain asset classes. Therefore, the risk is **likely.** **Known control activities and control gaps are as follows:** 1) The Risk Officer is currently in charge of monitoring the asset allocation against the approved asset allocation. 2) Currently, investment officers use excel spreadsheets to calculate impact on their respective regional portfolios, however, they do not have insight into the impact on the broader portfolio 3) Investment Officers need an attribution analysis tool in order to: a) know the broader impact of the investment management decisions b) monitor the impact of their decisions or tactical allocations An RFP is out for this tool. Responses are being collected and the decision is targeted to be made by July 8th. 4) Alternative Investments and Real Estate groups manage portfolio risk through diversification by geography, structure, statutory, type of real estate, etc.	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	Pension Fund Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Operational	IMS	**22**	**Investment Performance Monitoring**	The investment policy outlines the strategic asset allocation of the pension assets, as well as ongoing performance monitoring criteria. Performance of investments should be continuously monitored as part of the fiduciary responsibilities of the plan sponsor. Unless investment performance is appropriately monitored, the Pension Fund may be adversely impacted.	Without appropriate performance monitoring, individual investment manager performance as well as the performance of the total portfolio cannot be appropriately managed, which may result in loss of assets. Therefore, the impact would be **high.** The risk is **possible** because appropriate performance monitoring depends on use of appropriate information, benchmarks, and effective tools. **Known control activities and control gaps are as follows:** 1) Equity and Fixed Income groups may be using inappropriate benchmarks (or the benchmark monitoring tool may not be effective). 2) Real Estate group (Prospective Alternative Investment Group): a) Attends all meetings with investors to gain investment insight b) Participates in the respective investment advisory boards c) Influences fund investment strategy d) Monitors risk of re-financing assets and conditions of re-course e) May be unable to conduct performance reviews due to the lack of benchmarks for medium/high risk real estate investments f) There may be timing and currency differences between Northern Trust and Townsend reports as well as differences in currency calculation methods, which create challenges in reviewing performance. 3) For small cap investments, which are managed by external advisors, IMS Investments section performs quarterly monitoring of investment manager performance. IMS may take corrective action based on long-term underperformance. 4) Wilshire system is used to match performance information between Risk Officer & Investment Portfolio Managers. 5) Insufficient evaluation of recommendations from external advisors. 6) The benchmarks for investment performance monitoring are periodically revisited.	High	Possible	Average	Moderate Priority	Strengthen Preparedness	Management	Pension Fund Risk	1. Performance analytics are generated with input from the Investment Officers. 2. Performance analytics are limited in scope and granularity.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Operational	IMS	**23**	**Hedging**	Hedging activities can provide investment managers additional flexibility with regards to protection against loss or liability due to specified events and circumstances that may occur, or be discovered during a specified period. Pension funds that fail to undertake a comprehensive analysis of risk management strategies (including a detailed analysis of inherent risks associated with the assets and liabilities) may fail to manage the risks in an efficient manner.	Impact would be **medium** because an unmanaged exposure may result in loss of assets. The Pension Fund does not engage in hedging activities; however, the Pension Fund is focused on long term investments, possibly offsetting fluctuations throughout the life of the investment. Therefore, the risk is **possible.** **Known control activities and control gaps are as follows:** 1) The Pension Fund does not engage in additional foreign exchange hedging activities. 2) Contributions are impacted by currency fluctuations which are not always corresponding to the currencies of the benefit payments. 3) As the Pension Fund executes certain international investments, the currency risk may be somewhat hedged on an arbitrary basis. 4) The fund may not currently have the infrastructure to effectively engage in/manage hedging activities (i.e. staffing, expertise, systems, etc...). 6) Although the most recent asset liability study included an analysis of currency risk, an independent study has not been performed in recent years to determine whether or not hedging would benefit the Pension Fund.	Medium	Possible	Weak	Moderate Priority	Strengthen Preparedness	Management	Pension Fund Risk	1. Bottom up analysis required for each trade slows the execution of liquidations of investments in a country or region. 2. Currency risk management should be improved.
Program and project management	Operational	IMS	**24**	**Conflict of Interest - Internal**	Pension funds need an effective process to verify compliance of each investment professional and advisor with rules and regulations around possible conflicts of interest. Non-compliant activities may have a negative impact on the pension fund's reputation. Also, failure to accumulate accurate, relevant and reliable external and internal information to assess compliance may result in the issuance of misleading procedural guidelines and/or decisions.	Impact of this risk would be **high** because non-compliant Investment Officer activities would damage the reputation of the Pension Fund. The risk is **possible** because there are opportunities and incentives. **Known control activities and control gaps are as follows:** 1) A compliance policy is in place, which limits the personal trading opportunities for Investment Officers (buy/sell), based on the date of the same Pension Fund investments. However, there is no tracking system to validate that the Investment Officer's personal trades are not in violation of the trading window. 2) There is an annual disclosure requirement for all Pension Fund staff. Investment Officers are not required to disclose the activities throughout the year (only at year end). UN Staff Financial Disclosure Compliance reviews are performed by PWC. PWC also has access to Northern Trust records to review Investment Officer's holdings and trading history. 3) There is a restricted list of companies which may not be current. 4) Compliance Officer is responsible for reviewing compliance & investment officers' personal holdings. The Compliance Officer position has been vacant for several months. 5) There is a Code of Ethics for trading (which may not be relevant to investment activities) and compliance may not be monitored.	High	Possible	Weak	High Priority	Strengthen Preparedness	Management	Pension Fund Risk	1. Code of Ethics 2. Personal holdings and business activities disclosed by IMS personnel are not subject to independent verification by the UNJSPF.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Operational	IMS	**25**	**Conflict of Interest - External**	Pension funds need an effective process to verify compliance of each investment professional and advisor with rules and regulations around possible conflicts of interest. Non-compliant activities may have negative impact on the pension fund's reputation. Also, failure to accumulate accurate, relevant and reliable external and internal information to assess compliance may result in the issuance of misleading procedural guidelines and/or decisions.	The impact of this risk would be **high** because the Pension Fund may choose inferior investments based on the non-discretionary advisor's guidance. The risk is **likely** because: - there is a natural conflict of interest for advisors to trade the same advised fund - advisors may invest in a security and then provide advice to purchase security (front running). **Known control activities and control gaps are as follows:** 1) IMS monitors performance of advisors. 2) Indications of front running by third parties have been communicated to IMS. Such can directly reduce investment returns of the fund. 3) IMS is re-evaluating its current advisor structure. Management is in dialog with the Investment Committee to determine if another way of operating investment should be considered.	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	Pension Fund Risk	New
Program and project management	Operational	IMS	**26**	**Advisor Performance**	The investment advisors may fail to satisfy contractual requirements of delivering high quality information. The advisors may fail to meet the Pension Fund's expectations.	Discretionary advisors make their own investment decisions. The portfolio allocated to the discretionary advisors is not substantial (compared to the size of the overall portfolio), therefore the risk is somewhat limited, and the impact would be **medium.** Non-discretionary advisors provide information to the Investment Officers. The ultimate investment decision remains with the Investment Officer, mitigating the risk created by inferior investment advice, reducing the impact to a **medium** level. The risk is **possible** because advisors present to the Investments Committee, but are not responsible for their performance. **Known control activities and control gaps are as follows:** 1) IMS tracks the quality of external advisors' recommendations based on: a) Their presentations b) Economic analysis c) Activity & level of contact with the portfolio management, etc. d) Quality of idea generation 2) Quality of advisor recommendations are evaluated based on the following: a) Timeliness b) Appropriate research c) Alignment with the Pension Fund's investment strategy. 3) External advisor contracts can be terminated within 30 days; however, contracting a new advisor may take a long time due to the lengthy procurement process and the Pension Fund may lose opportunities as a result.	Medium	Possible	Average	Low Priority	Verify Preparedness	Management	Pension Fund Risk	1. The performance review of Investment Officers and external advisors (discretionary and non-discretionary) is not structured in a consistent manner.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Operational	IMS	**27**	**Internal Controls over Investments**	The Pension Fund has a fiduciary responsibility to ensure that assets are managed and monitored appropriately. Failure to consciously manage risks and implement necessary controls around the investment management activities can result in unauthorized use or loss of assets. Control activities must be implemented consistently with a focus on the rules and regulations, and long term objectives. Further, it is essential that unusual conditions identified as a result of performing control activities are investigated and appropriate corrective action be taken.	If appropriate internal controls are not incorporated into the investment management process, the Pension Fund may lose assets. Therefore, the impact would be **high.** Currently, the Pension Fund has several manual processes, and relies on the Custodian's internal controls. Therefore, the risk **possible.** **Known control activities and control gaps are as follows:** 1) All settlements are done by the custodian. Risk Management group monitors exception reports to ensure custodian's compliance with DvP (Delivery versus Payment) rule. The Pension Fund maintains a contract with the custodian, resulting in the custodian being held to the DvP rules. The Legal Officer is involved in contract review of custodian. 2) DTC confirmations are obtained manually. Faxes sent to and from the brokers are approved manually and sent to the custodian. 3) Northern Trust exception reports are only spot-checked for compliance. There is no independent cross reference/check or review of Northern Trust end of day reports. 4) The Risk Management officer currently oversees the risk management processes and provides input during trade operations; this may represent a conflict of interest. 5) All trades must have two authorizing signatures to be processed. 6) Settlements are segregated from the trading operations (Omega is used as the trading platform that allows monitoring trades). 7) IMS should only have view access to the holding records for decision making purposes; modification access should be restricted.	High	Possible	Average	Moderate Priority	Strengthen Preparedness	Management	Pension Fund Risk	1. Operations, Legal and Risk Management should be included on a continuous basis in all discussions of possible new investment products. 2. Ensuring compliance with ownership limits and restrictions is a manual process monitored by the Investment Officers. 3. Approved trades can be executed over a three month time frame.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Operational	IMS	**28**	**Investments Process Efficiency**	Inefficient processes may be a result of many factors, including outdated technology, expanding operations, and any changes in fund structure. Processes should be continuously monitored to ensure they are optimized and there is no unplanned redundancy. Performance of the Pension Fund can be negatively impacted when it adopts (or fails to improve) inefficient processes and this may have a cascading affect on operations.	Efficiency of processes is critical, especially for Investments sections. Although the Pension Fund would still be able to carry out its operations, the impact of inefficient processes is **high** because inefficiencies would result in high administrative costs or opportunity costs. Inefficient processes may also have a negative impact on employee morale. The risk is **likely** because certain processes (e.g. the current trading operations process) are manual. **Known control activities and control gaps are as follows:** 1) The Pension Fund has a plan to replace the current manual (fax based) trade order system with Charles River. The current fax based system does not allow standardized imbedded instructions. Charles River will have imbedded instruction capabilities. 2) The IMS Accounting section does not have visibility to transactions performed by Investment Officers in advance to get prepared for the volume. 3) IMS & PECSS have manually intensive procedures. 4) IMS is implementing Charles River. IMS is targeting to complete the implementation by the end of 2009.	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	Pension Fund Risk	1. Execution of a trade cannot take place until the written analysis is received from the external advisor. 2. The roles and authorities of the various bodies involved in the investment process should be clarified. 3. The cumbersome committee structure governing the UNJSPF complicates the communication of current activities in the portfolio and follow-up on specific initiatives.
Program and project management	Operational	Secretariat	**29**	**Communication of PECSS Requirements**	Pension entitlement requirements need to be communicated to all Member Organizations and participants, who must understand those requirements as well as their significance in implementation. Appropriate communications are required to ensure that day-to-day procedures adhere to the requirements.	This risk impacts the PECSS section. Lack of appropriate communication and understanding of PECSS procedures and documentation requirements by the Member Organization Staff Pension Committees (SPCs) or participants may result in: - delays in processing - negative impact on reputation Impact would be **low** because there are other controls over the documentation. The risk is **likely** because the SPCs are responsible for collecting documentation on behalf of the Pension Fund and provide Pension Fund related information to participants at their respective Member Organization. Also, SPCs are not subject to the authority of the Pension Fund; therefore, they may not understand or be responsive to the internal procedures of PECSS. **Known control activities and control gaps are as follows:** 1) There are booklets issued by the Pension Fund. 2) There is no central information repository that the SPCs and participants may use to get updated information about PECSS procedures and documentation requirements. SPC staff turnover rate is high. Therefore, an up-to-date reference guide may be prudent.	Low	Likely	Average	Low Priority	Re-evaluate Impact of Combined Risks	Management	UN Specific Risk	1. Member organizations' staff turnover, training and expertise

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Operational	Secretariat	**30**	**Changing Rules and Regulations**	The rules and regulations of the Pension Fund changes from time to time. Such changes may have a downstream impact on the administration of benefits, or require certain procedures and the program logic of the pension entitlements system to be updated. Failure to update the program logic accurately may result in inaccurate calculations, payments or litigation.	Impact would be **high** because, if the procedures and program logic is not updated accurately and timely, the PECSS may: - process inaccurate calculations - process over/under payments - incur additional costs for recovery - damage its reputation The risk is **possible** because the regulations are complex and changes from time to time. **Known control activities and control gaps are as follows:** 1) There is limited analysis to review the impact of the proposed recommendation to justify the request of the change before it is presented to the Pension Board. The Advisory Committee on Administrative and Budgetary Questions (ACABQ) may provide input. 2) Chief of Operations attends all meetings of the Pension Board, thus mitigating risk that provisions are adopted without full understanding of downstream impact on operations of the Pension Fund. 3) There is a recommendation that during implementation of IPAS, there will be no change in plan provisions and regulations. 4) Recommendations may place an administrative burden on the Legal Department. 5) PECSS personnel perform user acceptance testing on system updates. 6) User Acceptance Testing and Change Management Procedures were formally implemented in October 2008 and have not been reviewed by OIOS.	High	Possible	Average	Moderate Priority	Strengthen Preparedness	Management	UN Specific Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Operational	Secretariat	**31**	**Workload Planning**	Anticipating fluctuations in volume may permit the Pension Fund to plan their workload needs in a timelier manner. Absence of workload planning could prevent the Pension Fund from making resource allocation decisions on a more proactive basis.	Without appropriate workload planning, the Pension Entitlement and Client Servicing section may: - fail to meet demand for benefits processing - hinder meeting the benchmarks - damage its reputation The impact would be **medium.** The risk is **possible** because number of participants and pensioners/beneficiaries are increasing at a higher rate than the human resources available to administer the Pension Fund. There was a 53% growth in the last 10 years. Also, there are fluctuations due to separations (e.g. liquidating regions for peace keeping operations, for which participants must be separated at the same time after the mandate is complete). **Known control activities and control gaps are as follows:** 1) Copies of documentation are accepted while processing liquidating regions to expedite the process. 2) Benefits Officers may all take vacation at the same time. Management makes every effort to avoid such scheduling conflicts. 3) PECSS personnel do not have time allocated to administrative tasks (e.g. training subordinates, internal audits, implementing recommendations, etc). 4) PECSS may not have foresight to anticipate the volume of new participants. 5) PECSS has generally met its benchmarks in the past.	Medium	Possible	Average	Low Priority	Verify Preparedness	Management	UN Specific Risk	New
Program and project management	Operational	Secretariat	**32**	**Pensioner or Beneficiary Fraud**	The Pension Fund may fail to carry out checks on eligibility, or controls may be circumvented, before providing benefits. The Pension Fund may also fail to develop policies with respect to acceptable methods of payment, types of verification documents considered valid, or methods of establishing and validating the identity of the pensioner/beneficiary. Such control weaknesses may be exploited by pensioners/beneficiaries. Similarly, rules and regulations of the Pension Fund may be exploited by those who may try to receive overpayment or payment without eligibility.	The PECSS may make payments to illegitimate pensioners/beneficiaries. The impact would be **low** because fraud would likely be perpetrated on case by case basis. The risk is **possible** because opportunity exists due to the nature of the validation process and multiple languages. Incentives exist due to financial gain by the pensioners/beneficiaries. Also, PECSS relies on SPCs for document verification and has no control over how these documents are verified. **Known control activities and control gaps are as follows:** 1) A certificate of entitlement must be completed every year and signatures are authenticated. Thresholds to authenticated signatures were established (i.e. system flag for age for audits of certification of entitlement process) 2) PECSS only accepts original documents. In cases of liquidating regions, when the volume is high, PECSS may accept copies of documents instead of originals which are subsequently verified. 3) PECSS depends on the SPCs to provide accurate documentation and ensure that participant is eligible. 4) The Pension Fund cannot access death records in most countries.	Low	Possible	Average	Low Priority	Re-evaluate Impact of Combined Risks	Management	Pension Fund Risk	1. Cash payments to the appropriate person

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Program and project management	Operational	Secretariat	**33**	**Internal Controls over Pension Entitlements and Client Servicing**	The Pension Fund has a responsibility to ensure that payments are processed accurately and within the established timeliness. Failure to implement necessary controls can result in a lack of confidence that business goals will be achieved. Control activities must be implemented consistently with a focus on the rules and regulations and long term objectives. Further, it is essential that unusual or non-recurring conditions identified as a result of performing control activities are rectified through investigation and appropriate corrective action.	If PECSS processes inaccurate payments, the Pension Fund may experience loss of assets and reputation. The impact would be **high.** The risk is **possible** because the rules and regulations and pension entitlement and calculation process is complex. Therefore, the PECSS heavily relies on experience and internal controls. **Known control activities and control gaps are as follows:** 1) Index numbers are used for participants; however, one participant may have duplicative primary ids (e.g. rehiring retirees). To ensure accuracy of data, other information may be used such as names, birth date, etc. 2) Member organizations submit a personal action upon employee separation. At the time of separation, the Pension Fund changes the pension number to a "Separation Number" to suspend contributions. 3) PECSS performs a reconciliation of all entitlements with changes to the transaction in PENSYS 4) Entitlement process is not started until all documents are collected from Member Organizations. All documents must be stamped, including original payment instructions. 5) COLA and foreign exchange rate information are manually entered during payment. 6) There is a reconciliation of checks printed to payment requests. 7) Prior audits on complex cases discovered errors, resulting in a need for recovery activities. 8) Overpayment is recovered from survivor's beneficiary. If there are no survivors, Client Service suspends the benefits. Overpayments may be reported to the Pension Fund by the bank, beneficiaries of the deceased or the member organization	High	Possible	Strong	Low Priority	Verify Preparedness	Management	Pension Fund Risk	1. Manual intervention is required when country of residence changes for two track payments and when cost of living adjustments are necessary. 2. Payments continuing after death 3. Timely Reconciliations 4. Retirement Processing Compliance 5. Lawson Accounting System 6. Payment Processing
Program and project management	Operational	Secretariat	**34**	**Pension Entitlements and Client Servicing Process Efficiency**	Inefficient processes may be a result of outdated technology, growing operations, and changing fund structure. Processes should be continuously monitored to ensure that there is no unplanned redundancy. Performance of the Pension Fund can be negatively impacted when it adopts or fails to update inefficient processes that have a cascading affect on all its operations.	Efficiency of processes is critical for the PECSS section. The impact of inefficient processes is **medium** because the Pension Fund would still be able to carry out its operations; however, inefficiencies would result in high administrative costs or opportunity costs. Inefficient processes may also have a negative impact on employee morale. The risk is **likely** because the current pension entitlements and payments process is case by case. **Known control activities and control gaps are as follows:** 1) The PECSS initiated projects to move from a "case by case" approach, to a "process oriented" approach by implementing IPAS, which will allow: a) Member organizations to be able to provide participant and pensioner/beneficiary information faster b) The PECSS may be able to decrease turnaround time The Pension Fund is approximately 12-24+ months from actual IPAS implementation. 2) IMS & PECSS have manually intensive procedures.	Medium	Likely	Average	Moderate Priority	Verify Preparedness	Management	Pension Fund Risk	1. Performance turnaround times 2. Relationship between the New York office and the Geneva office.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Human resources management	Human Resources	Secretariat & IMS	**35**	**Succession Planning**	The Pension Fund may fail to use succession planning as a tool to develop and maintain strong leadership and ensure that skills and competencies, built while managing the complex processes of the Pension Fund, are transferred to successors.	Poor succession planning may result in: - loss of institutional knowledge, - inability to continue operations due to vacant posts, and - deteriorating employee morale due to challenges in adapting to increased responsibilities. Therefore, the impact would be **high.** The risk is **likely.** Mandatory retirement age requires experienced personnel to leave the Pension Fund. Completely customized in-house supported systems and processes prevent organization from hiring external talent with relevant pension entitlement, payment and client servicing experience. Currently, PECSS staff specialization takes on average 4-5 years.Current IMS talent pool only includes entry level professionals who are interested in gaining experience through the diverse portfolio of IMS, or tenured professionals who would prefer to work under lower performance goals and job security. Therefore, vacancies due to retirement or advancement of employees are difficult to fill. **Known control activities and control gaps are as follows:** 1) Succession planning is the responsibility of the manager. 2) IMS has started addressing this by building the investment management team. The portfolio managers have hired additional assistants who can assume their responsibilities in case the investment manager were to leave the Pension Fund. 3) Exceptions to mobility are granted for occupational groups (Investment Officers and Benefit Officers) which reduce the likelihood of loss of institutional knowledge with loss of experienced personnel. 4) UN rules and regulations require that vacant posts should to be announced and filled in by candidates from the UN organization. Therefore, even if the manager trains his/her direct report, the direct report may not be able to fill in the manager's post.	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	Business Risk	1. Upcoming Senior Management retirements 2. Upcoming IT Senior Management retirements 3. Not all positions have current job descriptions
Human resources management	Human Resources	Secretariat & IMS	**36**	**Training**	The Pension Fund may fail to direct, plan, and operate training and development programs. Absence of training may result in a reduction of relevant knowledge in professional, technical, or other fields that might be related to an employee's responsibilities. The Pension Fund may fail to achieve its mission and goals by not improving individual and, ultimately, organizational performance. There may not be a strategic approach that articulates priorities and invests in training and development to achieve strategic objectives.	Impact would be **medium,** as on the job experience is more critical in order to perform daily operations in PECSS and IMS. The risk is **likely** because UN in-house training programs are not applicable/ topic specific to Pension Funds. **Known control activities and control gaps are as follows:** 1) A learning management program has been initiated to create courses with procedures and material relevant to fund. 2) PECSS personnel do not have time allocated to facilitate training. Also, there is no specific group of personnel dedicated to training. 3) OHRM Training Catalog is in line with the UN goals and operations, not with the relevant IMS material. 4) Although there is a large budget for other trainings, it is not always accessible to attend, due to varying rules and regulations. 5) Insufficient Training Material related to Knowledge Management.	Medium	Likely	Average	Moderate Priority	Verify Preparedness	Management	Business Risk	1. Training

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Human resources management	Human Resources	Secretariat & IMS	**37**	**Talent Retention**	Poor or ineffective talent management in the Pension Fund might result in failure to attract and retain skilled candidates, or to fill open positions with the best people. The Pension Fund may fail to implement a competency-based talent management policy. Talent management decisions may not be driven by organizational core competencies as well as role- or position- specific competencies such as knowledge, skills, experience, and personal traits.	Impact would be **high** because poor talent retention may result in disruption in operations, loss of institutional knowledge and incurring additional cost of replacing personnel. The risk is **remote** because: - UN's working conditions and benefits attract and retain talent, - Staff is often appreciative and supportive of the culture of the UN, - Turnover is low. **Known control activities and control gaps are as follows:** 1) There is a competitive benefits package. 2) A cost of living adjustment is done every year to wages based on the current cost of living. 3) IMS has difficulty competing with compensation levels of Wall Street. 4) Inability to fill professional posts from within the department due to limitations of recruitment methodology may cause employee dissatisfaction. 5) UN Rules for promotion inhibit the ability of the departments to promote qualified professionals.	High	Remote	Strong	Low Priority	Verify Preparedness	Management	Business Risk	New
Human resources management	Human Resources	Secretariat & IMS	**38**	**Recruitment**	The UN's recruiting process may fail to identify a sufficient base of suitable candidates for open positions. The overall process may not address current and future project needs, determine if there are suitable internal candidates to fill positions, move candidates through the process efficiently, and eventually fill open positions with a strong candidate. Also, the process may not utilize all available and appropriate means for identifying candidates.	Impact would be **high** because open posts may hinder the operations of the Pension Fund.The risk is **likely** because: - UN Finance Officers may apply to work for the Pension Fund; however, external pension experts might not be aware of the available UN Pension Fund posts - UN recruitment process typically takes as long as one year, and therefore may not be able to fill a positions up to 1.5 years **Known control activities and control gaps are as follows:** 1) The Pension Fund follows the UN's OHRM rules; however, OHRM's policies and practices do not fit the Pension Fund's needs. 2) There is a need to recruit people to G4 level rather than G3. Otherwise pension fund recruits at too low level and cannot terminate employees to balance the workforce. 3) Occupational groups (investment and benefits officers) are not recognized as posts in Galaxy. These posts need to be entered as Finance or IT posts. 4) There is an initiative to put Senior Managers through assessment centers rather than standard UN recruitment panel process	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	Business Risk	1. Understaffing 2. The mix between permanent staff and contractors may expose the IMS to high personnel costs with inconsistent levels of redundancy.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Human resources management	Human Resources	Secretariat & IMS	**39**	**Performance Management and Accountability**	The Pension Fund may not always properly measure and monitor performance and implement incentive programs that motivate and reward its personnel for superior performance. Performance management programs typically include operational performance metrics, behaviors, competencies and adherence to policies. The Pension Fund may fail to implement compensation and incentive programs that reward performing employees appropriately and support retention programs.	Impact would be **high** because the Pension Fund may not reach its objectives due to poorly qualified staff performing pension entitlement and investment activities. Also, poor performance management would lower employee morale due to unmerited promotions. The risk is **likely** because the current performance management process is not relevant for the Pension Fund. **Known control activities and control gaps are as follows:** 1) Rules for promotion do not match with investment management necessities (attainment of CFA, etc.). Investment Officers are evaluated based on benchmarks. If benchmarks are not relevant, Investment Officer performance may not be evaluated appropriately. 2) UN promotion structure and regulations are not relevant: a) The EPAS evaluation process is not a priority. b) Goals established in the EPAS are not previously planned. c) UN policies do not facilitate terminating underperforming employees. 3) Capability of EPAS to add job specific competencies may not be consistently used.	High	Likely	Average	High Priority	Strengthen Preparedness	Management	Business Risk	New
Information and Systems Management	Information Resources	IMS	**40**	**IMS IT Strategy Alignment**	There is a critical dependence on technology to initiate, record, and manage all aspects of the Pension Fund's transactions and information. Failure to develop, acquire, and implement technologies that are aligned with the Pension Fund's strategies may result in the Pension Fund not fully achieving its objectives.	A lack of effective strategies and long-range information systems plans can result in: - Information systems not being supportive of the Pension Fund, - Management lacking confidence in the ability of information systems to support and add value to the Pension Fund, and - Information systems not operating as effectively and efficiently as possible. Therefore, the impact related to an ineffective technology strategy is **high.** The risk is **possible** since there is an informal process for developing and maintaining the IT strategy within IMS. **Known control activities and control gaps are as follows:** 1) The IMS IT Strategy is not documented. 2) There is no formal process for approving the strategy. 3) The current IMS IT strategy involves utilizing technology to more effectively support the Investment Management Services department by replacing manual processes with more automated processes based on real time transaction processing. Legacy systems may be replaced within the year (2009).	High	Possible	Average	High Priority	Strengthen Preparedness	Management	Business Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	IMS	**41**	**IMS Business Continuity and Disaster Recovery**	Inability to recover from business interruptions that cause critical information resources to be inoperative may adversely affect the Pension Fund's operations. Unless a business continuity plan includes a restoration strategy as part of a disaster recovery plan to return operations to normality, whether in a restored, remote or new facility, the Pension Fund may not be able to recover from business interruptions due to unforeseen events or incidents.	The Pension Fund's business continuity plan should be an integrated strategy to respond to unplanned interruptions to operations, providing timely resources that are required for critical processes. Without such a plan, restoration of processes may be delayed, and the Pension Fund may incur unnecessary financial losses in the event of an emergency or other unplanned interruptions. The impact is **medium** for the current system since IMS is not heavily reliant on application systems and critical IMS functions can be performed without the system. However, the impact will be high once the Charles River and SWIFT systems are implemented since the Investment Management Services department will be more reliant on information systems which will perform real-time transaction processing. The risk is **possible** because of the inherent nature of outside threats to the UN and the location of the processing environment. **Known control activities and control gaps are as follows:** 1) IMS has a documented disaster recovery plan in place to support its legacy systems (e.g., Omega, Abacus); which allows for "cold" site restoration of IMS legacy application systems. However, this may not be a sufficient restoration plan for the new investment systems (i.e., Charles River, and SWIFT). These applications will have the ability to execute trades electronically and in real time, placing more reliance on their availability. As such, the time required to restore the new application systems in the event of a disaster will be more critical. 2) IMS does not have a clearly defined and documented business continuity plan. 3) A formal business disaster impact assessment has not been performed to assess the needs of the Pension Fund and ensure the appropriate IT recovery or continuity plan is developed. 4) Once SWIFT is implemented IMS will be unable to execute trades if the system becomes unavailable. The impact would increase if it is down for more than 2 hours or the disruption occurs at the end of the trading day (e.g., around 3pm). 5) The Pension Fund may not have sufficient resources to implement recovery and business continuity plan in the event of a disaster and/or total system failure.	Medium	Possible	Average	Low Priority	Verify Preparedness	Management	Business Risk	1. Disaster recovery and business continuity plans do not exist.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	IMS	**42**	**IMS Systems Implementation**	The Pension Fund may encounter difficulty in implementing selected technologies. Implementation issues may include data conversion between different, sometimes incompatible platforms or difficulty in analyzing data. Implementation issues may result in inaccurate calculations, unreliable processing, incomplete recording of data, and disruption of operations.	Without sufficiently designed and implemented system implementation policies and procedures the Pension Fund may face: - Incomplete and inaccurate processing and recording of transactions - Loss of data during to the consolidation of Pension Fund records and Custodian records Due to the relative importance of Investment Management applications to the related processes, the impact would be **high.** The risk is **likely** because the Pension is planning to implement Charles River and SWIFT applications. There are inherent risks associated with such complex and challenging system implementations. **Known control activities and control gaps are as follows:** 1) IMS does not have any formal "Application System Implementation and Maintenance" policies and procedures. Formal policies and procedures ensure that new system implementations and/or additional modifications are performed consistent with management's intention. Without formal policies and procedures the following may not be sufficiently designed: a) A detailed implementation project plan. b) Sufficient testing. c) A "Go Live" check list. d) Problem/error tracking and resolution procedures. e) Training for end users. 2) The IMS IT department consists of approximately 5 individuals, which may result in difficulties supporting the implementation. 3) There is no project management software.	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	Business Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	IMS	**43**	**IMS IT Change Management**	Lack of adequate change control procedures, such as access controls, supervisory reviews, approval of change requests, documentation, impact analysis, and segregation of duties (migration from test to production environment by an independent group not involved in programming), may result in unauthorized changes being introduced into the production environment. Implementation of unauthorized, unapproved, or inappropriate changes into a production environment may damage the functionality of the Pension Fund's production systems.	The impact is **high** as the new IMS application systems will support time sensitive, real-time transaction processing. Without appropriate change management procedures, the Pension Fund may process incomplete and/or inaccurate transactions. The risk is **possible** because of the potential frequency and significance of changes. Changes to new application systems will be in the form of vendor released patches, fixes, upgrades, etc. IMS IT will not have access to source code for the new systems and will not be able to make custom changes. **Known control activities and control gaps are as follows:** 1) IMS does not have any formal "Application System Implementation and Maintenance" policies and procedures. This may result in lack of sufficient procedures to ensure that changes to existing systems are performed consistent with management's intention. The following procedures may not be sufficiently designed: a) Process to approve change requests. b) Clearly defined test plans (e.g., interface testing, unit testing, parallel testing, capacity testing, user acceptance testing, etc.). c) Documented results of test plan execution. d) Management approval prior to production implementation. 2) Management has frozen the legacy application environment due to the upcoming implementation of the new systems (i.e., Charles River and SWIFT). As a result, IMS IT will not be making changes to legacy systems.	High	Possible	Weak	High Priority	Strengthen Preparedness	Management	Business Risk	New
Information and Systems Management	Information Resources	IMS	**44**	**IMS Information Security**	An inability to secure data, information, applications, networks, and operating systems through appropriate logical and physical access controls may expose The Pension Fund's assets to threats such as malicious attack or damage, intrusion, and manipulation. Logical access can be protected by using access control software for authentication and identification of users and having appropriate access rules for authorizing transactions, log-in IDs and passwords, or biometrics. Weak physical access controls may allow unauthorized individuals to enter information processing facilities and access sensitive information and systems.	The impact of unauthorized access to new investment management systems (Charles River and SWIFT) and other IT systems is **medium** because of their increased role in supporting the investment management operations. The risk of unauthorized access to investment management and other IT systems is **possible** because of the importance of information maintained in these systems. **Known control activities and control gaps are as follows:** 1) There are no formal information security policies such as: a) Security configuration for new and existing systems. b) User account administration. c) A segregation of duties review. 2) User access and segregation of duty reviews are not performed. 3) IT does not receive timely notifications of users no longer requiring access (e.g., HR is not required to notify IT of terminations).	Medium	Possible	Weak	Moderate Priority	Strengthen Preparedness	Management	Business Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	IMS	**45**	**IMS Records Retention**	Risk exists if there are not a clearly articulated, documented records retention policies and procedures approved by counsel. Absent such a policy, the Pension Fund places itself at risk for non-compliance, as well as a risk of being unable to retrieve critical information, records, or data in event of a need to do so.	The impact of the IMS being unable to retrieve critical data is **medium,** since the majority of critical IMS information is retained in hard copy format due to the manual nature of current processes. This risk is **possible** since retention requirements have not been defined by end users and/or general counsel and the retention of critical data are dependent on the manual scanning of hard copy documentation. **Known control activities and control gaps are as follows:** 1) The IMS IT Department has not been provided with clearly defined requirements for the retention of electronic records and information. Data owners together with legal counsel have not established such requirements. This could result in information not being appropriately retained according to the Pension Funds' requirements or information being retained unnecessarily. 2) Application data is retained indefinitely. Lack of data retention policy may lead to archiving of unnecessary documents. Users may not be able to easily access important documents. 3) Restoration of application data backups are performed periodically during disaster recovery testing (tested in 2008). 4) There are instances where records are maintained in hard copy format (e.g., Townsend reports are all manual) rather than electronic.	Medium	Possible	Average	Low Priority	Verify Preparedness	Management	Business Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	IMS	**46**	**IMS IT Outsourcing**	The Pension Fund may contract with an outsourced vendor to perform part or all of the activities typically performed within the Pension Fund's computer processing environments. Typically, such contracts will include a formal service level agreement, which is designed to ensure that the outsourced vendor provides an appropriate level of service to the Pension Fund. Such service level agreements often include, but are not limited to, availability of access to the network, system response times, and turnaround time for problem resolution. The contract often provides a mechanism for measuring performance against the service level agreement and reporting those results to management of the Pension Fund. Failure to monitor the level of service provided and to take appropriate action may result in control deficiencies and/or inefficient or ineffective operations.	In July of 2009, IMS will be implementing new application systems (i.e., Charles River, SWIFT). The IMS department is planning to have these new applications hosted by IMSS, which will be responsible for the application systems supporting infrastructure (e.g., application and database hardware, operating systems). Because of this arrangement it is critical for IMS and IMSS to have an established Service Level Agreement (SLA) that clearly states the goals of service level agreements based on defined standards. Without a clearly defined, documented, and monitored service level agreement between IMS and IMSS, the following key items may not be appropriately established: - Clear definition of information system services required. - System performance and uptime requirements. - Problem management and escalation standards. - System configuration and security definitions. - Data retention requirements. - Reporting of key performance and service objectives. - Disaster recovery/business continuity planning. This may adversely impact system availability, data integrity, and overall user satisfaction; therefore, the impact is **high.** The risk is **likely** as the hosting arrangement is the first of its kind between the parties. **Known control activities and control gaps are as follows:** 1) The Pension Fund is working towards, but has not yet developed and documented a detailed hosting arrangement. 2) The IMSS department may not have sufficient resources to support the new application system (e.g., IMSS department may not have Sun Solaris Unix expertise as their current Unix environment is exclusively IBM AIX). 3) The hosting arrangement is the first of its kind for the IMSS department and may pose challenges during execution (e.g., adherence to hosting service level agreement, procedural changes may be needed to meet hosting requirements, the support of different technologies). 4) Service levels for the new system environment will need to be maintained at a high level given that the applications will have a more critical role in IMS business processes (e.g., execution of trades, real time transaction based).	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	Business Risk	1. IT Organization

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	Secretariat	**47**	**IMSS IT Strategy Alignment**	There is a critical dependence on technology to initiate, record, and manage all aspects of the Pension Fund's transactions and information. Failure to develop, acquire, and implement technologies that are aligned with the Pension Fund's strategies may result in the Pension Fund not fully achieving its objectives.	A lack of effective strategies and long-range information systems plans can result in: - Information systems not being supportive of the Pension Fund, - Management lacking confidence in the ability of information systems to support and add value to the Pension Fund, and - Information systems not operating as effectively and efficiently as possible. Therefore, the impact related to an ineffective technology strategy is **high.** The risk is **possible** since a number of the Pension Fund's applications currently do not fully meet the objectives of the business users. Furthermore, the IPAS project will not only entail implementing a major technology platform change but also changing the requirement of the system (i.e., how it is utilized). **Known control activities and control gaps are as follows:** 1) The Pension Fund's IT strategy is reviewed and approved by the funds IT steering committee and executive committee. Projects are reviewed monthly. 2) An independent review was performed in 2008 to provide an objective assessment of the Pension Fund's functions and structure. This also included identifying the risks associated with implementing IPSAS and recommendations for addressing such risks. 3) The majority of processes within the fund are manual intensive and do not effectively utilize information technology. 4) The fund has stated the need for replacing key systems such as PENSYS within the next four to five years. 5) There are numerous manual interventions in the payment process, benefit calculation process, and audit process.	High	Possible	Strong	Low Priority	Verify Preparedness	Management	Business Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	Secretariat	**48**	**IMSS Business Continuity and Disaster Recovery**	Inability to recover from business interruptions that cause critical information resources to be inoperative may adversely affect the Pension Fund's operations. Unless a business continuity plan includes a restoration strategy as part of a disaster recovery plan to return operations to normality, whether in a restored, remote or new facility, the Pension Fund may not be able to recover from business interruptions due to unforeseen events or incidents.	The Pension Fund's business continuity plan should be an integrated strategy to respond to unplanned interruptions to the operations and that provides for timely availability to resources required to operate critical processes. Without such a plan, restoration of processes may be delayed, and the Pension Fund may not be able to meet its benchmarks and in the event of an emergency or other unplanned interruptions, resulting in loss of reputation. The impact of an unplanned interruption to the fund is **high** due to the importance of timely processing of benefits (e.g., check processing). The risk is **possible** because of the inherent nature of outside threats to the UN and the location of the processing environment. **Known control activities and control gaps are as follows:** 1) The Pension Fund does not have a clearly defined and documented business continuity plan. 2) The IMSS department does have a disaster recovery plan for critical IT systems supporting the Pension Fund. Restoration of the PENSYS systems is the responsibility of the UNICC and involves restoration at a recovery site in Europe. The fund's accounting system (i.e. Lawson) and document imaging repository (i.e. Compliance) are processed in New York and have "Hot Site" recoverability at the UNICC data center. 3) Testing of the disaster recovery plan has been performed by the UNICC (2x a year). The restoration of the PENSYS application is tested yearly. Testing of the restoration plan for critical systems maintained by the IMSS outside of the UNICC data center has not been performed (i.e. Lawson, Compliance). 4) A formal business impact analysis has not been performed that would ensure IT identifies all critical IT functions that would need to be restored (e.g., network, email, # of users able to connect to restoration site). 5) Business continuity planning over payroll seems to be established.	High	Possible	Average	Moderate Priority	Strengthen Preparedness	Management	Business Risk	1. Operations 2. Disaster recovery and business continuity plans do not exist.

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	Secretariat	**49**	**IMSS Systems Implementation**	The Pension Fund may encounter difficulty in implementing selected technologies. Implementation issues may include data conversion between different, sometimes incompatible platforms or difficulty in analyzing data. Implementation issues may result in inaccurate calculations, unreliable processing, incomplete recording of data, and disruption of operations.	The impact for not having a controlled process for implementing new systems (i.e., IPAS/ERP) is **high.** An unsuccessful implementation may result in incomplete and inaccurate processing and recording of participant information, pension entitlements and payments. The risk is **possible** because the Pension is planning to implement IPAS. There are inherent risks associated with such complex and challenging system implementations. **Known control activities and control gaps are as follows:** 1) System development methodology is available and required to be adhered to. 2) Quality assurance policies have recently been developed, however the effectiveness of their implementation need to be evaluated and tested. 3) An independent review was performed in 2008 to provide an objective assessment of the Pension Fund's functions and structure. This also included identifying the risks associated with implementing IPSAS and recommendations for addressing such risks. 4) Replacement of the PENSYS system will be a significant undertaking that will require dedicated and experienced resources. The relative small number of IMSS staff may make it difficult to identify these resources. 5) Replacement of the PENSYS system with the IPAS system could be 12 to 24+ months in the future. It is still unclear as to the certainty of milestone dates. 6) Currently, there is no project management software. 7) There is an expected attrition of highly experienced IT resources in the application development group.	High	Possible	Weak	High Priority	Strengthen Preparedness	Management	Business Risk	1. PENSYS Infrastructure 2. Business Process Improvements

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	Secretariat	**50**	**IMSS IT Change Management**	Lack of adequate change control procedures, such as access controls, supervisory reviews, approval of change requests, documentation, impact analysis, and segregation of duties (migration from test to production environment by an independent group not involved in programming), may result in unauthorized changes being introduced into the production environment. Implementation of unauthorized, unapproved, or inappropriate changes into a production environment may damage the functionality of the Pension Fund's production systems.	The impact is **high** as the PENSYS application supports complex processes and transactions. Without appropriate change management procedures, the Pension Fund may process incomplete and inaccurate transactions. Without appropriate change management procedures, the Pension Fund cannot ensure that changes on PENSYS are in line with management's intentions. The following may be experienced: - Developers may make direct modifications to the production environment (e.g., no segregation of duties). - Monitoring of sensitive access may not occur (e.g., access to data and application source code). - Emergency changes may be made in the production environment without sufficient monitoring. - Sufficient testing of application changes may not occur as developers are designing the test plans (e.g., lack of an independent quality assurance (QA) function). - End user testing may not be sufficient to meet management's requirements. The risk is **likely** because of the potential frequency, significance and complexity of changes. **Known control activities and control gaps are as follows:** 1) System development methodology is available and required to be adhered to. 2) All changes are logged in a change management system. 3) Version control software is utilized to manage source code changes for the PENSYS application. 4) Quality assurance and segregation of duties policies have recently been developed; however the effectiveness of their implementation needs to be evaluated and tested. 5) Application developers make direct modifications to the application code within the production environment. 6) Application developers make direct modifications to the financial data within the production environment. 7) Policies and procedures for making emergencies changes are not designed and implemented. 8) There is no formal quality assurance function. 9) Monitoring controls over developers with access to production have not been implemented.	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	Business Risk	1. IT Staffing Levels

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	Secretariat	**51**	**IMSS Information Security**	An inability to secure data, information, applications, networks, and operating systems through appropriate logical and physical access controls may expose The Pension Fund's assets to threats such as malicious attack or damage, intrusion, and manipulation. Logical access can be protected by using access control software for authentication and identification of users and having appropriate access rules for authorizing transactions, log-in IDs and passwords, or biometrics. Weak physical access controls may allow unauthorized individuals to enter information processing facilities and access sensitive information and systems.	The impact of unauthorized access to PENSYS and other IT systems is **high** because of the complex calculations and private data maintained by these applications. The risk of unauthorized access to PENSYS and other IT systems is **possible** because of the importance of information maintained in these systems. **Known control activities and control gaps are as follows:** 1) Dedicated Information Security Officer. 2) Security policies have been implemented for a number of areas and others are in the process of implementation (e.g., Segregation of duties, user access reviews). 3) Key IT functions within the IMSS Department are not sufficiently segregated (e.g., developers have the ability to directly modify the production environment). 4) Developers have the ability modify production data. 5) Sufficient logging and monitoring of sensitive IT access and data may not be in place. 6) User access and segregation of duty reviews are not performed. 7) IT may not receive timely notifications of users no longer requiring access (e.g., HR is not required to notify IT of terminations). 8) User maintenance functions may not be sufficiently performed (e.g., role creation, modification, and maintenance and assignment of access outside of predefined/approved roles, etc). 9) Security monitoring and incident response procedures have not been developed (e.g., a list of critical tasks and the associated order of importance in which they are addressed). ***Note:*** Management is aware of many of the items above based on the OIOS review in12/08, and is 50% complete with implementing the recommendations.	High	Possible	Average	Moderate Priority	Strengthen Preparedness	Management	Business Risk	New
Information and Systems Management	Information Resources	Secretariat	**52**	**IMSS Records Retention**	Risk exists if there are not a clearly articulated, documented records retention policies and procedures approved by counsel. Absent such a policy, the Pension Fund places itself at risk for non-compliance, as well as a risk of being unable to retrieve critical information, records, or data in event of a need to do so.	The impact of the IMSS being unable to retrieve critical data is **high** due to the fact this may hinder payment processing, participant benefit calculation and pension case processing. This risk is **possible** since retention requirements have not been defined by end users and/or general counsel and the retention of critical data are dependent on the manual scanning of hard copy documentation. **Known control activities and control gaps are as follows:** 1) The IMSS has not been provided with clearly defined requirements for the retention of electronic records and information. Data owners together with legal counsel have not established such requirements. This could result in information not being appropriately retained according to the Pension Fund's requirements or information being retained unnecessarily. 2) Application data is retained indefinitely. Lack of data retention policy may lead to archiving of unnecessary documents. Users may not be able to easily access important documents. 3) Restoration of application data backups are performed periodically during disaster recovery testing.	High	Possible	Average	Moderate Priority	Strengthen Preparedness	Management	Business Risk	1. Data Security for Pension Fund Participants and Beneficiaries

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	Secretariat	**53**	**IMSS IT Outsourcing**	The Pension Fund may contract with an outsourced vendor to perform part or all of the activities typically performed within the Pension Fund's computer processing environments. Typically, such contracts will include a formal service level agreement, which is designed to ensure that the outsourced vendor provides an appropriate level of service to the Pension Fund. Such service level agreements often include, but are not limited to, availability of access to the network, system response times, and turnaround time for problem resolution. The contract often provides a mechanism for measuring performance against the service level agreement and reporting those results to management of the Pension Fund. Failure to monitor the level of service provided and to take appropriate action may result in control deficiencies and/or inefficient or ineffective operations.	The impact of not having a clearly defined, documented, and monitored service level agreement (SLA) between the IMSS and the United Nations International Computer Center (UNICC) is **high** since it could adversely impact system availability, data integrity, and overall user satisfaction. Without a well defined and monitored SLA, the following key items may not be appropriately established: - Clear definition of information system services required. - System performance and uptime requirements. - Problem management and escalation standards. - System configuration and security definitions. - Data retention requirements. - Reporting of key performance and service objectives. - Disaster recovery/business continuity planning. The risk is **remote** due to the maturity of the relationship and static nature of the scope of services received. **Known control activities and control gaps are as follows:** 1) The responsibilities of the UNICC and the IMSS are established in a formal service level agreement. 2) The IMSS monitors the level of services provided. 3) The UNICC has had performed by an independent auditor a control evaluation of its information technology environment that supports the PENSYS applications.	High	Remote	Strong	Low Priority	Verify Preparedness	Management	Business Risk	New

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	Secretariat & IMS	**54**	**Data Integrity**	There is a risk if the Pension Fund data is not accurate and complete; or protocols are not in place to assure standardized handling during any use or access (such as transfer, storage or retrieval); and, that data is not protected for its intended use.	The Pension Fund requires complete, accurate, and valid data in order to perform its required functions. The impact of incomplete, inaccurate, and invalid data is **high** due to the overall importance to the Pension Fund (e.g., benefit funding, actuarial analysis). In addition, "clean" data is critical for the successful future implementation of IPAS. The risk of data integrity issues is **likely** based on the following: - Numerous data transfers occur into the PENSYS system increasing the chances of synchronization issues. - Data transfer error resolution and reconciliation procedures are not effectively designed to ensure data integrity. - Member Organizations' Human Resource departments are not held accountable for the accuracy of data transferred into the PENSYS system. - Data in the PENSYS system is directly modified in the production environment by IT developers. **Known control activities and control gaps are as follows:** 1) There are numerous and redundant manual controls at various levels throughout the pension benefit process. 2) 75% of the Human Resources related files transferred from Member Organizations into PENSYS are processed by an automated interface. 3) 20% of the finance related files transferred from Member Organizations into PENSYS are processed by an automated interface. 4) No escalation procedures are in place to ensure the timely resolution of data transfer errors. 5) Annual reconciliations are not performed to ensure that the data within the PENSYS system is synchronized with local member organizations. 6) The manual process for ensuring the accuracy of currency exchange rate and consumer price index information may not be sufficient. 7) The security over sensitive and confidential data related to the data collection process may not be sufficient. 8) Application developers have the ability to make direct modifications within production. 9) As a consequence of the data integrity issues the Pension Fund relies on redundant and manual controls to mitigate data integrity risks over benefit calculations. This has resulted in inefficiencies. 10) There may be a risk that a retiree's pension amount could be modified without proper review or approval. (See follow up question). 11) Inaccurate Human Resources data in the PENSYS system could affect actuarial estimate. Currently, the fund will validate Human Resources data in PENSYS when an employee retires.	High	Likely	Weak	High Priority	Strengthen Preparedness	Management	Pension Fund Risk	1. Data integration with member organizations

Focus Area	Risk Category	Department	#	Risk Name	Risk Description	Assessment Details	Impact	Likelihood	Preparedness	Overall Rating	Action	Responsibility	Prevalence	Previous Risk Name/ Description
Information and Systems Management	Information Resources	Secretariat & IMS	**55**	**Privacy**	Unauthorized access to personally identifiable information (PII) creates a significant risk. Dissemination of personally identifiable information can have a negative effect on stakeholders. Protecting PII requires appropriate data classification, which is the conscious decision to assign a level of sensitivity to data as it is being created, amended, enhanced, stored, or transmitted. The classification of data and documents is essential to differentiate between that which is not sensitive to disclosure and that which is highly sensitive and confidential. The risk exists if data is stored, received, created, or amended without appropriate security and ownership.	This impact of unauthorized access to sensitive data (including PII) is **high** as a result of its potential for: - Damage to relationships with key stakeholders (e.g., UN reporting entities, plan participants). - Cost of litigation. - Damage to reputation. - Loss of productivity (effort to investigate and remediate). The risk is **possible** since there is uncertainty as to the volume of sensitive information being maintained by the Pension Fund and the current safeguards over such data. **Known control activities and control gaps are as follows:** 1) No process exists for data owners to assess and classify the sensitivity and confidentiality of data within the Pension Fund including data relating to personally identifiable information (PII). Without this classification the IT function is unable to ensure sensitive electronic information is properly secured. Further, it becomes impossible to monitor whether such data has been compromised. **Note:** Data governance policies including standards for data classification are in development. 2) There is a clean desk policy at PECSS. 3) Data is not encrypted on user laptops, desktops, and personal digital assistants (PDA's), however projects are underway to address this. 4) IT development staff is assigned powerful system rights providing them the ability to view and edit production data. 5) Electronic distribution of reports utilized within the Pension Fund is not encrypted nor is there a clear understanding as to the sensitivity of the information (due to the lack of data ownership). 6) There is no defined approach for responding to data privacy breaches (i.e., unauthorized access to sensitive/PII data). 7) Outsourced shredding company to destroy confidential documents.	High	Possible	Weak	High Priority	Strengthen Preparedness	Management	Business Risk	1. Data Security for Pension Fund Participants and Beneficiaries