September 2012

| | | | | | | |
|---|---|---|---|---|---|---|
| | منظمة الأغذية<br>والزراعة للأمم<br>المتحدة | 联合国<br>粮食及<br>农业组织 | Food and<br>Agriculture<br>Organization<br>of the<br>United Nations | Organisation des<br>Nations Unies<br>pour<br>l'alimentation<br>et l'agriculture | Продовольственная и<br>сельскохозяйственная<br>организация<br>Объединенных<br>Наций | Organización<br>de las<br>Naciones Unidas<br>para la<br>Alimentación y la<br>Agricultura |

# COUNCIL

## Hundred and Forty-fifth Session

## Rome, 3-7 December 2012

## Review of Enterprise Risk Management in the United Nations System (JIU/REP/2010/4)

1. This JIU Report is accompanied by brief comments of the Director-General and more extensive joint comments of the UN system Chief Executives Board (CEB) for Coordination (UNGA A/65/788/Add.1).

*Comments from the Director-General of FAO*

2. FAO endorses the CEB comments and is pleased to report that it is in the process of addressing Recommendations 1 and 2.

3. The nine benchmark practices for ERM proposed under Recommendation 1 have been included in the design of FAO's approach to ERM[1]. FAO regularly reports to its governing bodies progress on implementation of ERM and the management of major risks as advocated in Recommendation 2.

4. FAO also supports Recommendation 3.

[1] FC 135/13; FC 138/12

United Nations A/65/788/Add.1

General Assembly

Distr.: General
17 August 2011

Original: English

**Sixty-fifth session**
Agenda items 128 and 135

**Review of the efficiency of the administrative and financial functioning of the United Nations**

**Joint Inspection Unit**

# Review of enterprise risk management in the United Nations system

## Note by the Secretary-General

The Secretary-General has the honour to transmit to the members of the General Assembly his comments and those of the United Nations System Chief Executives Board for Coordination on the report of the Joint Inspection Unit entitled "Review of enterprise risk management in the United Nations system: benchmarking framework" (see A/65/788).

*Summary*

The report of the Joint Inspection Unit entitled "Review of enterprise risk management in the United Nations system: benchmarking framework" assesses the risk management practices in place in United Nations system organizations and proposes a collection of benchmarks that agencies can apply when implementing a risk management framework.

The present note presents the views of United Nations system organizations on the recommendations provided in the said report. The views of the system have been consolidated on the basis of inputs provided by member organizations of the United Nations System Chief Executives Board for Coordination, which welcomed the comprehensive review of risk management. Agencies generally accepted the recommendations, although they expressed some reservations regarding several of the benchmarks.

# I. Introduction

1. The report of the Joint Inspection Unit entitled “Review of enterprise risk management in the United Nations system: benchmarking framework” (see A/65/788) examines the concept of risk management and its relevance to United Nations organizations, assesses the risk management practices and experiences within the United Nations system and proposes a collection of benchmarks that agencies should apply when implementing a risk management framework.

# II. General comments

2. Members of the United Nations System Chief Executives Board for Coordination (CEB) welcomed the report and expressed appreciation for its comprehensive approach to a difficult subject. They recognized the importance of enterprise risk management in almost every facet of an organization’s operations and were of the view that a well-structured approach to risk could help their organizations deliver on their mandates. Agencies noted, and generally accepted, the three recommendations contained in the report, which were focused on the implementation of the 10 benchmarks considered as best practices for enterprise risk management. However, agencies noted some concerns with several of the benchmarks.

# III. Specific comments on recommendations

**Recommendation 1**
**Executive heads should adopt the first nine benchmarks set out in this report, with a view to ensuring that the enterprise risk management approach is accepted and implemented in line with best practices.**

3. While generally supportive of recommendation 1, agencies also indicated concern regarding benchmark 6, which recognizes that the successful implementation of enterprise risk management requires adequate funding, a view that agencies strongly support. However, agencies noted the challenge of identifying dedicated resources for enterprise risk management projects, especially in an environment of limited budget flexibility. In addition, since many of the other benchmarks depend on resources, whether financial or human, agencies may experience difficulties in fully implementing the benchmarks. Agencies noted that the Joint Inspection Unit, in paragraph 115 of the report, considered a situation in which resources might become constrained and further noted that some agencies had been able to make progress without extensive funding. However, agencies wished to convey both the limitations of proceeding without appropriate resources and the consideration that, for many agencies, ensuring adequate resources to introduce enterprise risk management and sustain the implementation process, as stated in the benchmark, may go beyond the mandate of executive heads as, in general, legislative bodies determine funding allocations.

**Recommendation 2**

**Governing bodies should exercise their oversight role regarding the adoption of enterprise risk management benchmarks set out in this report, the effectiveness of implementation and the management of critical risks in their respective organizations.**

4. Agencies noted that recommendation 2 was addressed to legislative bodies and welcomed the potential role of those bodies in supporting the development of comprehensive enterprise risk management processes within their agencies.

**Recommendation 3**

**The CEB, through the High-level Committee on Management, should adopt benchmark 10 of this report, with a view to facilitating inter-agency cooperation, coordination, knowledge-sharing and the management of common and cross-cutting risks for more effective and efficient risk management throughout the system.**

5. Agencies supported recommendation 3, albeit with some reservations. This recommendation calls for the High-level Committee on Management to implement benchmark 10 (inter-agency cooperation and coordination, including the development of a common enterprise risk management framework, knowledge-sharing mechanisms and management of common and cross-cutting key organizational risks). Agencies agreed that there was merit in creating an informal network of risk practitioners across the United Nations system to share knowledge and experience; however, the remainder of the recommendation (i.e. to develop a system-wide risk universe based on unified standards, policies, frameworks and practices) might prove challenging for the system to achieve, particularly given the lack of homogeneity of operations and mandates across agencies. CEB members suggested that such an approach might distract from the higher priority of designing, implementing and embedding an approach to risk management that meets the particular needs of each United Nations body. Nevertheless, agencies agreed that a coordinated approach would prove useful, especially as many agencies appeared to be in the early stages of enterprise risk management development.

JIU/REP/2010/4

Original: ENGLISH

# REVIEW OF ENTERPRISE RISK MANAGEMENT IN THE UNITED NATIONS SYSTEM

## Benchmarking Framework

*Prepared by*

***Cihan Terzi***
***Istvan Posta***

**Joint Inspection Unit**

**United Nations, Geneva 2010**

# EXECUTIVE SUMMARY

## Review of enterprise risk management in the United Nations system: Benchmarking framework JIU/REP/2010/4

*Objective*

The objective of the study was to review enterprise risk management (ERM) policies, practices and experience in the United Nations system, and to identify best practices and lessons learned.

The review aimed to provide balanced information and recommendations in the following areas: (a) the concept of ERM and its relevance to United Nations organizations; (b) an assessment of ERM practices in the United Nations organizations; (c) best practices from the United Nations system and other organizations; (d) basic definitions of some risk management concepts and the methods of implementation; and (e) inter-agency cooperation, coordination and knowledge sharing in the United Nations system.

*ERM and its relevance to United Nations organizations*

ERM is an essential element of good organizational governance and accountability. It is a systematic and organization-wide approach, which supports an organization’s achievement of its strategic objectives by proactively identifying, assessing, evaluating, prioritizing and controlling risks across the organization.

The objective of ERM is to help ensure the sustainability of an organization and enable it to meet its organizational objectives. ERM requires the implementation of an organization-wide risk management process; makes risk management the responsibility of everyone; and provides a coherent methodology for its implementation.

During recent decades, the expansion of the mandate and operations of the United Nations organizations, coupled with unstable environments, has resulted in an increasing volume and complexity of risks encountered by these organizations. In addition, United Nations organizations inherently face unique challenges, such as a wide range of mandates and limited resources, a complex organizational structure and lengthy decision-making process, many objectives and lack of capacity, and reform backlogs. As a result, organizations face a risk climate that is growing increasingly more complex and prone to significant operational surprises.

*ERM implementation in the United Nations system*

Overall, United Nations system organizations are at the beginning stages in terms of the adoption and implementation of ERM. The progress is slow and depends on ad hoc decisions rather than an adopted formal plan. Many organizations are either preparing policy and framework documents or undertaking pilot/first phase exercises. The United Nations Development Programme (UNDP), World Food Programme (WFP), International Fund for Agricultural Development (IFAD), and International Maritime Organization (IMO) are relatively advanced in ERM in comparison to other organizations; however, their implementation is still immature and yet to be integrated into organizational processes and culture. Several organizations are yet to consider ERM.

The reasons for the slow adoption and progress of ERM in the system are many, such as: a lack of collective understanding and commitment by senior management; lack of a formal implementation plan; uncertainty about how to implement and integrate ERM into organizational processes; lack of an appropriate governance structure to support implementation; and the pressure of competing reform initiatives. In addition is the fact that as ERM is a relatively new management tool and is still evolving, organizations are trying to find their way in relatively uncharted territory.

Inter-agency cooperation and coordination are yet to be fully explored. It is clear that while it is necessary to adjust the ERM approach according to the specific nature of each organization, there is a need for a system-wide approach so as to ensure the speaking of a common language within the system on ERM; the identification and management of key common and cross-cutting risks (e.g. safety and security and reputational risks); avoidance of duplication; and optimal use of scarce resources.

Effective oversight by governing bodies is generally lacking. In view of the importance of having an effective risk management process, and the strategic implications of critical risks, it is imperative that governing bodies should exercise their oversight role.

*ERM benchmarking framework*

Based on the review of ERM literature, experience and lessons learned, the inspectors have identified 10 JIU benchmarks for the successful implementation of ERM in United Nations organizations. The inspectors believe that if the organizations follow these benchmarks, and in addition senior management understand the importance of ERM and engage with the implementation, and utilize best practices, lessons learned, and expertise within the system, they will make quick progress in the successful implementation of ERM.

The first nine benchmarks laid out in the report should be adopted and implemented as a package by each executive head to ensure successful ERM implementation in their respective organizations. Benchmark 10, which requires inter-agency cooperation and decision, should be discussed and adopted at the level of the United Nations Chief Executives Board for Coordination (CEB). As the Chairman of the CEB, the Secretary-General of the United Nations should pursue the implementation of the recommendation addressed to CEB.

**Recommendations**

1. **Executive heads should adopt the first nine benchmarks set out in this report with a view to ensuring that the ERM approach is accepted and implemented in line with best practices.**

2. **Governing bodies should exercise their oversight role regarding the adoption of ERM benchmarks set out in this report, the effectiveness of implementation and the management of critical risks in their respective organizations.**

3. **CEB through the High-level Committee on Management (HLCM) should adopt benchmark 10 of this report with a view to facilitating inter-agency cooperation, coordination, knowledge sharing, and the management of common and cross-cutting risks, for more effective and efficient risk management throughout the system.**

## CONTENTS

## ABBREVIATIONS

| | |
|---|---|
| ACABQ | Advisory Committee on Administrative and Budgetary Questions |
| AICPA | American Institute of Certified Public Accountants |
| CEB | United Nations System Chief Executives Board for Coordination |
| COSO | Committee of Sponsoring Organizations of the Treadway Commission |
| CRO | Chief Risk Officer |
| ERM | Enterprise Risk Management |
| ERP | Enterprise Resource Planning |
| FAO | Food and Agriculture Organization of the United Nations |
| HLCM | High-level Committee on Management |
| IAEA | International Atomic Energy Agency |
| ICAO | International Civil Aviation Organization |
| ICSC | International Civil Service Commission |
| IFAD | International Fund for Agricultural Development |
| ILO | International Labour Organization |
| IMF | International Monetary Fund |
| IMO | International Maritime Organization |
| IPSAS | International Public Sector Accounting Standards |
| ISO | International Organization for Standardization |
| ITU | International Telecommunication Union |
| JIU | Joint Inspection Unit of the United Nations system |
| OECD | Organisation for Economic Co-operation and Development |
| OSCE | Organization for Security and Co-operation in Europe |
| RBM | Results Based Management |
| UNDP | United Nations Development Programme |
| UNEP | United Nations Environment Programme |
| UNESCO | United Nations Educational, Scientific and Cultural Organization |
| UNFPA | United Nations Population Fund |
| UN-HABITAT | United Nations Human Settlements Programme |
| UNHCR | Office of the United Nations High Commissioner for Refugees |
| UNICEF | United Nations Children’s Fund |
| UNIDO | United Nations Industrial Development Organization |
| UNODC | United Nations Office on Drugs and Crime |
| UNRWA | United Nations Relief and Works Agency for Palestine Refugees in the Near East |
| UNWTO | World Tourism Organization of the United Nations |
| UPU | Universal Postal Union |
| WFP | World Food Programme |
| WHO | World Health Organization |
| WIPO | World Intellectual Property Organization |
| WMO | World Meteorological Organization |

# I. INTRODUCTION

1. As part of its programme of work for 2009, the Joint Inspection Unit (JIU) conducted a system-wide review of implementation of Enterprise Risk Management (ERM) in United Nations system organizations from November 2009 to July 2010. The review had been suggested by UNESCO, UNFPA, and OIOS.

2. The objective of the study was to review ERM policies, practices and experiences in the United Nations system, and to identify best practices and lessons learned. It aims to provide balanced information and recommendations in the following areas: (a) the concept of ERM and its relevance to United Nations organizations; (b) an assessment of ERM practices in the United Nations organizations; (c) best practices from United Nations system and other organizations; (d) basic definitions of some risk management concepts and the methods of implementation; and (e) inter-agency cooperation, coordination and knowledge-sharing in the United Nations system.

3. The scope of the review covers all JIU-participating organizations, with a focus on those organizations that have either introduced ERM or are in the process of doing so (see annex III). The scope covers existing and planned ERM policies and practices within these organizations in line with established policies and practices in the private, public and multilateral sectors.

4. ERM is an essential element of good organizational governance and accountability. It is a systematic and holistic approach to risk management. It supports an organization's achievement of strategic objectives by proactively identifying, assessing, evaluating, prioritizing and controlling risks across the organization. As it assists the organization to better prepare for the future, and for uncertainty, it cannot be de-linked from planning and priority-setting mechanisms.

5. Through continuous horizon scanning and "what if" scenarios, it helps organizations reduce surprise risks, identify opportunities, and maintain the relevance and sustainability of their services. It is important to note that risk and opportunity are inseparable despite their different definitions. Effective risk identification techniques focus as much on opportunities as they do on risk, and failure to identify opportunities for the achievement of the organization's objectives is a risk in itself.

6. Over the years, United Nations organizations have increasingly adopted the ERM approach. The governing bodies of some organizations have been closely involved in the adoption of ERM, e.g. the General Assembly of the United Nations has passed ERM-related resolutions[1] and the Council of the International Maritime Organization (IMO) has established an intergovernmental working group for ERM implementation.

7. Comments from participating organizations on the draft report have been sought and taken into account in finalizing this report. In accordance with article 11.2 of the JIU Statute, this report has been finalized after consultation among the Inspectors so as to test its conclusions and recommendations against the collective wisdom of the Unit. The Inspectors wish to express their appreciation to all who assisted them in the preparation of this report, and particularly to those who participated in the interviews and so willingly shared their knowledge and expertise.

8. To facilitate the handling of the report and the implementation of its recommendations and the monitoring thereof, annex IV contains a table indicating whether the report is submitted to the organizations concerned for action or for information. The table identifies those recommendations

[1] General Assembly resolution 61/245, para. 3, and General Assembly resolution 64/259, paras. 30 and 31.

relevant for each organization, specifying whether they require a decision by the organization’s legislative or governing body, or can be acted upon by the organization’s executive head.

*Importance of ERM*

9. During the last decade, the collapse of some large private corporations and the impact of the recent major financial crisis have highlighted the critical importance of ERM as an instrument to manage and address critical risks within reasonable limits. Although initially developed in the private sector, more and more public entities, including United Nations entities, have started to consider how to integrate ERM into their business practices.

10. The objective of ERM is to help ensure the sustainability of an organization and enable it to meet organizational objectives. ERM requires organization-wide risk management policies and processes, and provides a coherent methodology for their implementation. Unlike traditional fragmented risk management practices, the concept of ERM embodies the notion that risk management cuts across the entire organization.

11. Private or public, no company or organization has the luxury of functioning in a risk-free environment. The nature of the mandates and services of United Nations system organizations are such that many organizations have to operate in complex and unstable environments, which, from the start, expose them to high risks. In particular, the development, humanitarian and peacekeeping-related activities of the organizations are inherently fraught with exposure to high risks. In 2009 alone, more than 30 United Nations staff members were killed in the line of duty coming under attack while providing humanitarian assistance.[2] It should be emphasized that ERM does not guarantee, but increases the possibility of the identification and treatment of important risks.

*Methodology and limitations*

12. The methods followed in preparing this report included a preliminary desk review which included the review of publicly available ERM literature, generic ERM frameworks and standards, and the experience of both private and public sectors. Questionnaires were sent to all JIU-participating organizations in order that an overview of ERM practices in the United Nations system could be obtained. On the basis of the responses received, the Inspectors conducted interviews with officials of the participating organizations.

13. Additionally, in order to identify best practices and lessons learned, the Inspectors conducted interviews with key officials from a number of non-participating United Nations and other international organizations, i.e., the International Fund for Agricultural Development (IFAD), the European Commission, the Global Fund, the Organization for Security and Co-operation in Europe (OSCE), the International Monetary Fund (IMF), the World Bank, and the Organisation for Economic Co-operation and Development (OECD).

14. ERM is a relatively new approach in the United Nations organizations. The lack of maturity of its implementation has not been conducive to identifying well-established and tested best practices. The Inspectors therefore strove to gather information from other international organizations and Governments that have implemented ERM for a relatively longer time. However, available funding did not allow for visiting many relevant organizations and locations. This was a constraint in the preparation of this report.

[2] See annual report of the Executive Director of UNICEF: progress and achievements in 2009 and report on the in-depth review of the medium-term strategic plan 2006-2013 (E/ICEF/2010/9), para. 181.

### *Evaluation Criteria: Benchmarking framework*

15. Based on the review of ERM literature, experience and lessons learned, the Inspectors identified the following elements as JIU benchmarks for the successful implementation of ERM in United Nations organizations:

Box 1: Benchmarks for successful ERM implementation

***JIU benchmarks for ERM:***

1. *Adoption of a formal ERM policy and framework.*
2. *Full commitment and engagement of executive management to leading the ERM strategy and implementation process.*
3. *Formal implementation strategy including a time-bound action plan and clear roles and responsibilities to manage the process.*
4. *Formally defined appropriate governance structure and clearly established roles and responsibilities for the implementation.*
5. *Communication and training plan to create risk awareness, promote risk policy and build up general capacity and critical skills for the implementation of ERM.*
6. *Provision of adequate resources to introduce ERM and sustain the implementation process.*
7. *Formal risk management process with coherent methodology and tools and clear guidelines for implementation.*
8. *Integration of risk management with RBM, planning, programming, and operational and business processes.*
9. *Monitoring, evaluation and reporting mechanisms to ensure compliance with and effectiveness of risk management.*
10. *Inter-agency cooperation and coordination including the development of a common ERM framework, knowledge sharing mechanisms, and management of common and cross-cutting key organizational risks.*

16. The assessment of the ERM practices in the United Nations organizations was based on the above-listed JIU benchmarks as key evaluation criteria, allowing a systematic assessment of whether ERM implementation by the organizations meet these best practice benchmarks. However, the report is not limited to this assessment; it also aims to provide multi-level information, such as explaining basic ERM concepts and methods and best practices in different areas.

# II. OVERVIEW OF THE ERM CONCEPT AND ITS RELEVANCE TO UNITED NATIONS ORGANIZATIONS

## A. ERM: Background, definition and benefits

*Background*

17. Risk is an event, the occurrence of which has the potential to influence the achievement of an organization's objectives.[3] An event can be positive or negative, an opportunity or a threat. Risk is measured in terms of impact and likelihood. Risk management is not an end in itself, but a means to an end, which is to achieve the goals of an organization.

18. Risk is a reality of all entities both in the commercial and public service sectors. Any entity which strives to achieve its goals/objectives inevitably has to manage uncertainty during its operations. Over decades, corporations have developed risk management practices in specific areas like safety, project management, portfolio management and business continuity. However, this traditional "silo approach" lacks consistency and scope, and misses the identification and holistic view of the key risk exposures potentially affecting an entity's ability to achieve its goals.

19. In the last decade, a number of big corporate scandals have highlighted the need for an enterprise-wide integrated and systematic approach to risk management. This approach is referred to as enterprise risk management or ERM. The most recent economic crisis, which has affected businesses, Governments and the public worldwide, has further illustrated the potential benefits of this approach, and the need for effective oversight by senior management, audit committees and boards of directors/governing bodies.

20. There is an emerging consensus among good governance experts that the ERM approach constitutes best practice in risk management. As a result, the adoption of ERM is gaining momentum among both commercial corporations and the public sector. ERM simply aims to identify and prevent obstacles, and exploit opportunities for achieving the objectives of an entity; therefore it works for any entity, be it commercial, not-for-profit or governmental, big or small. Research done through the Internet indicates that Government organizations of Australia, Canada, New Zealand, South Africa and the United Kingdom of Great Britain and Northern Ireland are already implementing ERM.

*Definition*

21. In line with increasing need and demand, during the last decade, a number of ERM principles, standards, frameworks and guidelines have been introduced into the international arena. They all have in common the concept that risk management should be overarching, structured, integrated and organization-wide. There are many definitions of ERM. In simple terms it can be defined as follows:

> *ERM is an organization-wide process of structured, integrated and systematic identification, analysis, evaluation, treatment and monitoring of risks towards the achievement of organizational objectives.*

[3] COSO, *Enterprise Risk Management Framework – Integrated Framework*, appendix E.

22. ERM, as a major element of strategic management, requires that risk management should be an explicit part of the accountability system. Ultimate accountability for risk management lies with executive heads and senior managers, while all managers and staff are responsible for managing risk.[4] In the past, risk management was implicitly part of the accountability system; the establishment of a formal ERM policy and procedures would rightly make it explicit.

23. The ERM concept raises risk management to another level, by linking the entire organization and all categories of risk. It responds to the need of governing bodies and management to understand an organization's portfolio of top risk exposures which might affect the organization's objectives. Its implementation would lead organizations to improve their situational awareness, which in turn would enable management to respond to risks more proactively.

24. A successful risk management approach should be proportionate to the level of risk (as related to the size, nature and complexity of the organization), comprehensive in its scope, integrated with organizational activities and processes, and dynamic, allowing for continuous updating, monitoring and improvement, and able to respond to changing circumstances.[5]

*Benefits*

25. ERM offers a coherent methodology for risk management, and protects and adds value to the organization and its stakeholders. Based on the review of literature, the benefits of ERM are summarized below:

Box 2: Benefits of ERM

(a) Makes risk management an integral part of achieving organizational objectives; thus helps ensure that those objectives are achieved.

(b) Improves management's ability to understand, identify and proactively manage risks.

(c) Improves planning, programming and decision-making and their implementation by ensuring a comprehensive and structured understanding of objectives, activities and related risks and opportunities.

(d) Reduces inefficiencies inherent in the traditional segmented risk management approach through overarching integrated risk management.

(e) Allows management to identify and prioritize key risks using an organization-wide portfolio view of risks.

(f) Optimizes organizational efficiency and protects and enhances assets and organizational image.

(g) Identifies common and cross-cutting risks and improves cross-departmental communication and discussions.

(h) Reinforces the accountability and integrated internal control framework.

[4] Australia, *Better Practice Guide – Risk management* (Barton, Department of Finance and Deregulation, 2008), p. 24.

[5] IRM, AIRMIC and Alarm, *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000* (2010), p. 3.

## B. Relevance of ERM for the United Nations system organizations

26. During recent decades, the expansion of the mandate and operations of the United Nations system organizations, coupled with unstable environments, has resulted in an increase in the volume and complexity of risks encountered by these organizations. Globalization, sophistication of business transactions, and the overall pace of change in operations and technology have contributed to the formation of a more dynamic risk environment. In addition, United Nations organizations are facing unique challenges, such as a wide range of mandates and limited resources, complex organizational structures and lengthy decision-making processes, many objectives and lack of capacity, and reform backlogs. As a result, United Nations organizations, in particular those organizations with a substantial field presence are facing a risk climate growing increasingly more complex and prone to significant operational surprises.

27. The interviews in United Nations organizations indicated that most officials recognize the benefit of implementing ERM, however a few officials, particularly from relatively small organizations, raised the following arguments against ERM for their organizations:

> “We already intuitively or informally manage risks, so we do not need this expensive private sector tool. Our organization is a small organization engaged in normative work so we do not have significant enough risks to justify using ERM”

28. Every organization has some form of risk management. The challenge, however, is that existing risk management practices are ad hoc, unsystematic and informal, leading to a lack of understanding and consideration of the main organization-wide risk exposures affecting the key goals that they seek to achieve. Additionally, the lack of an enterprise-wide ERM policy and procedures is not conducive to establishing accountability for risk management.

29. The ERM approach does not guarantee, but does strongly increase, the possibility of the timely identification and management of important risks. Moreover, properly implemented, ERM would increase efficiency and improve effectiveness through integrated risk management. A critical risk for any United Nations organization would be a risk that might cause a substantial failure in the organization delivering its essential services to fulfil its overall mandate. The ERM approach, through the systematic and organization-wide assessment of risks, would increase the possibility of identification and, hence, the treatment of those risks.

30. To give another example, with the traditional approach, risk assessment made for an Enterprise Resource Planning (ERP) project, if done, would stay within the executing department; whereas with the ERM approach, risks are escalated to corporate level if they are deemed to have a high probability and important impact on the operation of the organization. Thus, the ERM process would require the entire top management to consider the risk and ensure the allocation of resources to reduce the risk to a minimum.

31. It is a fact that all organizations, big or small, normative or operational, simply by their existence, have objectives to achieve and uncertainty that needs to be managed. Often, some main potential risks might already be known. An ERM approach formally recognizes these risks, ensuring that they are registered, discussed by senior management and assigned to the relevant officials to manage. Thus, ERM lays the foundation for accountability and responsibility for managing those risks; hence reinforcing the effective risk management in the organization.

32. The cost of ERM depends on the sophistication of the chosen ERM structure and tools. Not all organizations require very sophisticated risk management systems. The decision on the degree of technical complexity and which formalized governance structure best fit an organization will depend on the size and nature of the organization’s operations.

## III. IMPLEMENTATION OF ERM

*Overview of ERM practices in the United Nations system*

33. Annex III of this report summarizes the status of ERM implementation in United Nations organizations. The United Nations Development Programme (UNDP), the World Food Programme (WFP), IFAD and IMO are leading agencies in terms of ERM implementation. They have developed a significant level of ERM experience; however, their implementation is still immature and has not yet been embedded into business processes and organizational culture. Of these organizations, UNDP, IFAD and IMO have already embarked on full ERM implementation. Although WFP was the first organization to adopt an ERM policy in 2005, its full implementation has been delayed for various reasons. Officials explained that, although risk management at the operational level is better, it is still ad hoc and an overarching integrated ERM approach is lacking. They envisage embarking on implementing ERM fully starting in the second half of 2010.

34. The United Nations, the United Nations Educational, Scientific and Cultural Organization (UNESCO), the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), the United Nations Population Fund (UNFPA), the United Nations Children's Fund (UNICEF), the International Labour Organization (ILO), the Food and Agriculture Organization (FAO), the International Civil Aviation Organization (ICAO), the World Health Organization (WHO), the World Meteorological Organization (WMO), the United Nations Industrial Development Organization (UNIDO), the International Telecommunication Union (ITU) and the International Atomic Energy Agency (IAEA) are in the early stages of ERM implementation, either developing policy and processes, or performing training and introductory ERM practices (first phase or pilot).

35. The benefits of ERM are not yet tangible given the general lack of maturity of its implementation within the United Nations system. The impetus behind the decision to implement ERM in United Nations organizations usually originated in internal audit departments. External auditors and audit committees also played a role by recommending ERM implementation.

*Other organizations*

36. The Inspectors found that the European Commission is relatively advanced in ERM implementation in comparison to United Nations organizations. The Commission's risk management policy was introduced in 2005 in a pilot exercise. Despite having been in place for five years, officials consider that more time is needed in order for the European Commission to benefit fully. Other non-United Nations organizations that are progressing in ERM are OSCE and the Global Fund.

*Overall assessment*

37. Although it is easy to introduce generic ERM concepts and techniques, successful implementation has proved to be a real challenge, arising from the fact that effective ERM implementation is a function of the whole organization, not just one unit or group. ERM must be understood and embedded in the function of all units, business processes and operations.

38. According to a recent survey,[6] potential major impediments that entities face in considering ERM implementation are as follows: competing priorities; insufficient resources; lack of perceived value; lack of board or senior executive ERM leadership; and the perception that ERM adds bureaucracy. The Inspectors found that the same elements were among the leading impediments in the United Nations system.

39. Overall, the majority of United Nations organizations are either considering, or at the early stages of, ERM implementation. For the most part, risk management is still fragmented, unstructured, informal and implicit. Many of them have already developed risk management elements in certain areas, such as project management, security, information systems and business continuity; however, they lack integrated organization-wide risk management. Lack of full ERM implementation inevitably leaves executive heads and governing bodies without enough and timely information regarding the organizations' top risk exposures, including in governance and overall management.

40. Most of the officials interviewed in the United Nations organizations see the value of ERM, yet its adoption and implementation are slow in practice. For instance WFP introduced ERM policy in 2005 but implementation stalled until 2009. WFP officials explained that, due to downsizing and giving priority to International Public Sector Accounting Standards (IPSAS) and ERP projects, the implementation of a fully integrated ERM system was put on hold until 2010. The United Nations prepared a framework in 2008 but has not yet embarked on implementation. As seen in annex III, several organizations have not even started considering the issue yet.

### *Benchmark 1: Adoption of a formal ERM policy and framework*

41. Two fundamental challenges in risk management are to reach a common understanding of risk management, including the use of a consistent methodology and risk terminology throughout the organization; and to harmonize individual risk management practices by integrating them into an overarching organization-wide risk management process. Only a formal ERM policy and framework can overcome these challenges.

42. Among the organizations of the United Nations system, WFP, UNDP, UNICEF, ILO, UNESCO, ICAO, IMO, WHO, WMO, IFAD and IAEA have ERM policy and/or framework documents. FAO, UNRWA, and UNIDO are in the process of developing them.

43. United Nations organizations do not follow a standard approach in the development and adoption of ERM policy documents. Some organizations developed their documents internally, whereas others chose to employ consultants for that purpose. While in some organizations there is a formal management decision or decision by the governing body, in some others implementation has started on an informal basis without a formal adoption of the policy document.

44. Officials of the majority of organizations that have developed or are developing ERM policy and frameworks stated that their main reference is the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) ERM framework,[7] although they adjust the framework to

[6] Mark Beasley et al., *Report on the Current State of Enterprise Risk oversight*, 2nd ed. (American Institute of Certified Public Accountants (AICPA) and North Carolina State University, 2010). Available from http://mgt.ncsu.edu/erm/.

[7] COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (the Treadway Commission). The Treadway Commission was jointly sponsored and funded by five main professional accounting associations and institutes headquartered in the United States of America. These five organizations formed what is now called COSO.

the specific nature of their organizations. Most recently, in 2009, the International Organization for Standardization (ISO) published ISO 31000 Risk Management – Principles and Guidelines.

45. In essence, all available international frameworks have more similarities than differences. Officials should find the best approach for their organizations by reviewing available generic frameworks, and the policy and frameworks already developed in the United Nations system. In the preparation of policy documents it is important to establish a risk management philosophy and terminology, and provide the essential structure, methodology, guidance and tools for consistent implementation and governance of the process.

46. There is great variety in the structure, scope, content, quality, degree of detail, use of terminology and context in the available ERM documents in the United Nations system. UNICEF, UNDP, UNESCO and IMO documents provide relatively detailed information, including definitions, objectives, and implementation techniques, whereas most others provide a few pages of general information.

47. The Inspectors are of the view that there is great room for harmonization of ERM policy and framework documents in the United Nations system, including terminology, approaches and techniques. The Inspectors suggest that organizations draft their documents in accordance with internationally recognized professional terminology, frameworks and standards and, most importantly, in cooperation with each other.

48. The ISO definitions for risk management policy and framework are included in the box below.

Box 3: Definition of risk management policy and framework

- ➢ *Risk management policy* is a statement of the overall intentions and directions of an organization related to risk management.

- ➢ *Risk management framework* is a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization.
  - ▪ The foundations include the policy, objectives, mandate and commitment to manage risk.
  - ▪ The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities.
  - ▪ The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

*Source: ISO guide 73:2009, definitions 2.1.2 and 2.1.1*

*Business case*

49. In order to facilitate the adoption and introduction of ERM and explore possible strategies for its implementation, executive heads could prepare and utilize business cases, which should analyse the costs and benefits, establish necessary resources and justify the money to be spent, in developing and maintaining ERM. This approach would help to achieve management buy-in and act as a mitigating measure to the potential major impediments that organizations face in considering the adoption of ERM.

*Benchmark implementation indicator*

50. The Inspectors conclude that in order to implement benchmark 1, the executive heads of those organizations:

- That have not yet done so should prepare and introduce a formal ERM policy and framework with a view to establishing integrated, systematic, and organization-wide risk management.
- That have already adopted an ERM policy and framework should review and revise their policy and framework in the light of available international standards and best practices.

## *Benchmark 2: Full commitment and engagement of executive management to leading the ERM strategy and implementation process*

51. Experience indicates that ERM implementation largely depends on the understanding and ownership of executive/senior management. Executive heads and other senior managers are accountable for risk management and setting "the tone at the top". The commitment of senior managers demonstrated by regularly involving risk management processes in their respective areas of responsibility and promoting risk management in their daily use of language and actions is essential.

52. The Inspectors are of the view that insufficient understanding and commitment by senior management in United Nations organizations is one of the most common reasons for not adopting ERM, or the slow progress in its implementation. There are cases where one or only a few senior officials took ownership of and pushed the process, but when they left or their positions changed, ERM stalled. During interviews, it was not unusual to see that, although some officials were strongly in favour of ERM implementation, some other officials raised their doubts about the need for ERM. This reflects a lack of collective understanding and commitment at the top level, which is not conducive for successful implementation.

53. Experience shows that the full commitment from and engagement by top officials can be facilitated through focused presentation to and training of top officials regarding the ERM concept, its benefits and how to implement it. Furthermore, the business case for ERM can be utilized to promote it at the senior management level and throughout the organization. There is no doubt that executive heads have a critical role to play in fostering commitment and ownership at the top level.

*Benchmark implementation indicator*

54. The Inspectors conclude that in order to implement benchmark 2, executive heads should ensure that senior managers understand ERM and demonstrate their commitment and ownership by being actively involved and held accountable for the deployment of risk management strategies and implementation processes. The executive heads themselves should set "the tone at the top" and demonstrate with their words and deeds their full support for ERM.

## *Benchmark 3: Formal implementation strategy including time-bound action plan and clear roles and responsibilities to manage the process*

*Documented formal strategy and plan*

55. Experience shows that the successful introduction of ERM requires a well designed time-bound formal plan with a strategy/programme that includes steps and phases of implementation. Roles and responsibilities for implementing the strategy plan also need to be clearly established and

communicated. A formal project plan approach would lay the ground for accountability and sustained implementation. In the absence of a formal plan, ERM cannot be institutionalized and implementation would depend on the personal efforts of some managers, which would inevitably fade away when those managers leave or as time goes on.

56. One of the main reasons for the slow progress of ERM in the United Nations organizations is the lack of documented and time-bound formal implementation plans. In general, ERM introduction processes are fraught with ad hoc decisions. In some organizations plans existed; however, they were too general, or just outlined the intentions of officials rather than being a well documented and formally adopted programme.

*Gradual/phased versus simultaneous implementation*

57. For those organizations that have introduced ERM, a phased approach was usually chosen, with some variations in scope and speed. The only exception was UNDP, where ERM was introduced at both corporate and country level simultaneously by establishing risk registers. UNDP officials stated that, while corporate-level risk management and the use of corporate risk logs were relatively straightforward, risk management and the use of risk logs were problematic at the country level. Therefore, officials hesitated to conclude that simultaneous implementation worked well for them. Among other international organizations, the European Commission and OSCE both chose to follow a phased approach.

58. During interviews, many officials stated as a lesson learned that a successful approach to ERM implementation would be, as they dubbed it, “ERM light”: a simple approach to begin with, which can be built on as experience and knowledge are gained. As a starting point, some organizations chose administrative functions and gradually moved to programmatic areas; others held pilot exercises in headquarters and field offices.

59. Simultaneous organization-wide implementation usually requires more human resources and training to facilitate, and lacks the benefit of internal lessons-learned. While small organizations with strong senior management commitment and comprehensive early training of staff might benefit from simultaneous organization-wide implementation, a phased approach would be more useful to organizations with diverse operations and a field presence, both in terms of cost implication and the opportunity to build on experience. Nevertheless, the Inspectors caution that any approach has to be implemented with a documented plan.

*Competing reform initiatives: combined strategy*

60. One of the main reasons for the delay or slow progress of ERM implementation in the United Nations system is competing reform initiatives. It is a fact that United Nations organizations have recently embarked on multiple reform initiatives in which each reform requires a significant level of capacity, resources, attention and time of staff. During interviews, some officials stated that they believe in the value of ERM; however, there were competing reform initiatives, and as a result they suggested delaying ERM implementation. Others argued that IPSAS, ERP and results-based management (RBM) initiatives should be completed as a priority before taking up ERM implementation.

61. The Inspectors recognize that it is difficult to carry out major reforms simultaneously; however, the opportunity is there to integrate ERM easily into these reform initiatives and, moreover, ERM could be utilized to manage the risks of these reform processes. An integrated approach to multiple reform initiatives would create synergy, and increase the effectiveness and efficiency of all reforms. For instance, ERM could easily be integrated into the process of identification and achievement of objectives and expected results of RBM and, in fact, it should

be an imperative part of any organization’s strategic planning and monitoring process. In the case of an ERP project, the integration of some ERM modules into ERP from the beginning would save costs and improve the ERM process.

62. The Inspectors caution that pressing parallel reform initiatives should not be an excuse to delay ERM implementation: ERM should be part and parcel of all initiatives. However, given the fact that more resources would be needed, organizations should strive to gather together those necessary.

63. Among United Nations system organizations, UNICEF, UNFPA and UNIDO are planning an integrated approach to the introduction of ERM. The Inspectors were informed that ERM in UNICEF is being rolled out as part of the wider organizational improvement process, recognizing the links between ERM and other improvement initiatives such as: consolidation of the accountability system and regulatory framework; simplification of the programme result structure; business process improvement; organizational performance management system; ERP; and the adoption of IPSAS.

64. To facilitate an integrated approach, UNICEF and UNFPA have established chief risk management positions in their change management offices. UNICEF officials explained that the change management strategy was an organized means of introducing new initiatives and allowed for the integration of different subject matters into one training course. UNIDO envisages that ERM will be introduced in conjunction with their overall change management initiative, which includes business process re-engineering, implementation of a new ERP system and RBM. Thus, it will make it possible to avoid overlaps, ensure coherent development and give the best value for money.

*Benchmark implementation indicator*

65. The Inspectors conclude that in order to implement benchmark 3, executive heads should ensure that organizations have a formal organization-wide ERM strategy, including a time-bound action plan with steps and phases of implementation outlined and roles and responsibilities clearly assigned to manage the process. The strategy should explicitly be adopted and communicated across the organization.

## *Benchmark 4: Formally defined appropriate governance structure and clearly established roles and responsibilities for the implementation*

66. Once a decision has been made to implement ERM, the challenge for the organizations is to set up appropriate governance structures and determine roles and responsibilities in such a way that the implementation process works effectively, and the contributions of all players in terms of risk management can converge in a systematic and coordinated manner.[8]

### (i) Experience in the private sector

67. During the last decade, in the aftermath of corporate scandals and the financial crisis, risk management has gained an elevated importance in the good governance of corporations and the oversight role of boards of directors. Regulations in some countries have recently started requiring the disclosure of risk assessment measures.[9] In line with this development, boards of directors, in order to exercise their oversight role, have either strengthened the role of audit

[8] South Africa, *Public Sector Risk Management Framework* (National Treasury).

[9] Art. 663b, Swiss Code of Obligations.

committees or created special external risk committees. On the management side, executive heads have started creating high-level chief risk officer (CRO) positions and establishing internal risk committees.

*ERM committee*

68. While, in general, audit committees[10] are mandated to review the risk management practices of corporations, in order to have a better focus and expertise, corporations, particularly in the financial sector, have started establishing external risk committees. In a recent survey done in the banking sector, 35 per cent of banks reported that they had an external risk committee that is separate from the audit committee.[11] Another survey that included 700 entities from diverse sectors (AICPA and North Carolina survey)[12] found that, when boards of directors delegate risk oversight to a board-level committee, most (65 per cent) assign that task to the audit committee; and that 30 per cent of entities surveyed had internal risk committees that formally discuss enterprise level risks.

*Chief Risk Officer (CRO)*

69. CROs were first employed in the large financial corporations to deal with compliance issues, and their employment spread to other corporations faced with regulations such as "Sarbanes-Oxley" that require strict internal controls.[13] According to a survey done in the financial sector, 73 per cent of corporations surveyed had a CRO or equivalent position.[14] More than three quarters of the corporations surveyed indicate that CROs report to a board-level committee, the chief executive officer, or both. However, according to the AICPA and North Carolina survey that included entities from diverse sectors, only 23 per cent have created CRO positions. The survey results indicate that, currently, it is mostly large financial institutions, particularly banks, that choose to employ CROs.

### (ii) Experience in United Nations organizations and the European Commission

***ERM secretariat: risk officer***

70. In United Nations organizations there is no established dedicated high-level CRO position, division or unit for ERM implementation. In general, the leadership function for ERM is formally or implicitly delegated to risk committees, or senior management at large. A few organizations have chosen to employ dedicated staff as risk management expert/risk officer at the P-4 or P-5 level, in a so-called "ERM secretariat". Their function is to assist ERM implementation by providing technical knowledge. Other organizations chose or are planning to assign this task as a dual function, formally or informally, to one or more staff in one of the top-level offices, e.g. executive office and strategic planning and programming office.

71. UNDP has an ERM secretariat, comprising one full-time P-4 position, and residing in the operations support group of the Executive Office. In UNICEF, a chief risk management position

[10] In 2004, the New York Stock Exchange adopted rules that require audit committees of listed firms to oversee management's risk oversight processes.

[11] Grant Thornton LLP, *17th Bank Executive Survey* (2010), conducted in conjunction with *Bank Director* magazine.

[12] *Report on the Current State of Enterprise Risk Oversight.*

[13] Keith Regan, "Does your company need a chief risk officer?", *E-Commerce Times*. Available from http://www.ecommercetimes.com/story/43737.html.

[14] Deloitte, *Global Risk Management Survey: Sixth Edition – Risk management in the spotlight* (2009). The survey includes responses from 111 financial institutions worldwide with more than $19 trillion in total assets.

(P-5 level) was established in the change management office. The change management office reports to the Deputy Executive Director. UNICEF officials stated that the ideal location for central ERM coordination is in the office of the Executive Director, and it will be moved there once ERM is fully implemented.

72. In UNFPA, a senior risk advisor (P-5 level) has recently been placed in the change management and business continuity office, which is part of the Executive Office. In WMO, a strategic planning and risk management officer (P-5 level) has been appointed in the strategic planning office. In WHO, a P-5 level management officer in the Office of the Assistant Director-General for General Management supports the risk management process, in addition to other functions. In the case of WFP, officials explained that there have been difficulties in assigning full-time staff, as a result, most of the work was taken forward personally by the head of the Division for Performance and Accountability, with support from external consultants.

*European Commission practice*

73. As for non-United Nations organizations, the Inspectors note that, in the European Commission, there is no dedicated unit or risk officer for ERM implementation at central level. The Director General has the final responsibility for risk management in his/her Directorate-General. Internal control coordinators established in every Directorate-General play the role of catalyst in risk management. Depending on the size and complexity of activities, each Directorate-General decides whether the internal control coordinator is assigned full time for internal control and risk management issues. Officials stressed that a “catalyst” with the necessary expertise, initiative and motivation is important in keeping the risk management process alive. Furthermore, two central services of the European Commission are in charge of providing overall guidance on risk management and the management of cross-cutting risks.

***ERM committees***

74. UNDP, UNESCO, WFP, WMO and IFAD have internal risk management committees that consist of senior managers, whereas in other organizations it was assumed that senior management committees would perform that function. In general, ERM committees are tasked to review and monitor ERM implementation, give advice and/or make decisions on implementation strategies, and identify top level risks and guide the response.

75. In UNDP, the corporate ERM committee, chaired by the Associate Administrator, is responsible for ensuring that ERM is effective, relevant, and that the ERM process is applied consistently and systematically organization-wide. The committee meets on a quarterly basis and also decides on corporate risks and their treatment. It recently recommended that the discussion of corporate risks be integrated as a standing item on the agenda of the Operations Group each quarter. This group is chaired by the Associate Administrator with representation by Deputy Directors in all Bureaux. UNDP officials informed the Inspectors that the Operations Group will take on the role of the ERM committee accordingly.

76. The risk management committee in UNESCO is chaired by the bureau of strategic planning, with the secretariat provided by the internal oversight service. It supports the risk management process across the organization, and meets regularly on a monthly/bimonthly basis to discuss risk areas and develop action plans for mitigation. It reports to senior management and also to the oversight advisory committee.

77. In IFAD the Vice-President is identified as the lead executive responsible, and chairs the ERM committee. The committee is composed of the Vice-President as risk champion, the chief of finance and administration (acts also as the alternate chairperson), and senior representatives from

each department. The Director of Internal Audit and the General Counsel participate as observers. The role of the committee is to guide the development and implementation of ERM and to review and monitor ERM processes and outputs on a regular basis.

*IMO experience: intergovernmental ERM committee*

78. Among United Nations system organizations, only IMO has an intergovernmental ERM committee. It is somewhat similar to the external ERM committees found in the private sector. IMO's practice is defined briefly in the box below.

Box 4: IMO intergovernmental ERM working group/committee

> The IMO Council established an intergovernmental risk review, management and reporting working group/risk committee to develop a risk management system, oversee its implementation and to report to the Council regularly in the context of the organization's strategic and high-level action plans.
>
> Within the IMO secretariat, the policy and planning unit in the Office of the Secretary-General leads ERM implementation, supported by the administrative division and the internal oversight service. At the governance level, the lead lies with the IMO Council, supported by its risk committee.
>
> The ERM framework was approved by the Council, and the first risk assessment exercise concentrated on the deliverables of the secretariat. Officials informed the Inspectors that the Council had established a correspondence group to consider if risk management should also involve the deliverables of the membership/regulatory bodies.

79. IMO is – for the moment – a unique example whereby an organization has utilized the existing ERM expertise of Member States to develop an ERM policy without cost; and also where Member States have assumed their oversight responsibility effectively, by establishing a specific ERM working group with oversight and advisory functions. Officials explained that the direct engagement of Member States in the process was very positive and helped in developing and refining ERM; it also contributed to the understanding that ERM is not just a concern for the secretariat, but for the whole organization.

***Focal points/liaisons***

80. In UNDP, most units across the organization have risk focal points who are responsible for coordinating efforts to strengthen risk management. The role of risk focal point is rarely a distinct position; it is normally added to the responsibilities of existing staff. IMO and IFAD also use focal points. UNICEF risk policy defines the responsibilities of risk liaison officers/focal points clearly. The policy envisages that they may be planning officers, staff concerned with monitoring, evaluation or research, or other specialists.

### (iii) Assessment and conclusion: Optimal governance structure for United Nations organizations

*Private sector versus United Nations organizations*

81. As discussed above, the Inspectors conclude that there is no one-size-fits-all solution for ERM governance structure. Depending on the size, complexity, sector and risk profile of the entities concerned, the risk management function may range from a single risk champion and part-time risk officer, to a full-scale risk management department and high-level separate CRO. In view of the significant differences between private corporations and United Nations organizations, it would be inappropriate to copy the ERM structure of one to the other.

82. In the private sector, it is mainly financial corporations that have specific ERM structures, and they are usually much larger than United Nations system organizations in terms of budget and administrative and financial operations. In these corporations, risk-taking and financial risk is more prevalent, and CROs and risk committees are required to ensure compliance and keep these activities under control. They have inherently high financial risks which can endanger their very survival. In the public sector, operational risk is prevalent, the culture is mostly risk averse, and the risk management position is to promote responsible risk-taking. In the public sector, many organizations have difficulty in deciding on the correct structure and reporting lines for the risk management function.[15] The major difficulty therein is that risk management is not a stand-alone function: it embraces all aspects of the organization and has to be carried out by all organizational units. Therefore, the ideal structure and reporting lines are not immediately apparent.

83. During interviews, most officials expressed the opinion that there was no need for a heavy separate structure, because it may be perceived that risk management was entirely the responsibility of this dedicated structure, instead of all staff, and could lead to a stand-alone ERM exercise which would end up as bureaucratic paperwork with little benefit. In view of their findings, the Inspectors concur with this view that ERM should be built into, and not onto, an organization's management systems and practices. They conclude that, in general, United Nations organizations do not necessarily need an external ERM committee, dedicated large ERM units or separate high level CRO positions. However, as will be explained later, the Inspectors are of the view that a central ERM capacity to assist implementation (a secretariat), and a risk champion would greatly facilitate implementation.

*Emerging best practices*

84. Although there is no one-size-fits-all solution, there are emerging tendencies and best practices for the successful implementation of ERM. It is a key lesson learned that sustained and effective implementation requires a formal and appropriate governance structure, including strong leadership and coordination capacity at the corporate level. It is important to identify a senior level official to lead the organization's risk management policy and strategy, and to establish centralized capacity, e.g. a risk team or secretariat, to ensure successful ERM implementation. Organizations that demonstrate good risk management practice are those that have identified an individual or team to oversee the implementation of the risk management process.[16] Another emerging best practice is the assignment of focal points to facilitate risk management practice throughout the organization.

85. It needs to be emphasized that a formal ERM governance structure does not necessarily require a heavy new and additional governance layer in the organizations. However, accountability and responsibility for ERM must be clearly identified and formally assigned to players in the existing governance structure.

86. The decision as to the appropriate governance architecture depends on the level of value that ERM is required to deliver and the range and severity of risks to which the entity is exposed. Those organizations of a medium to large size with significant levels of risk exposure would require a high-level risk champion, though not necessarily working full-time as such, and a dedicated central risk management team/risk secretariat. Such teams would normally be responsible for general assistance in the implementation of ERM: technical support regarding the risks associated with mission critical initiatives and projects; maintaining a log of serious control

[15] South Africa, *Guidebook: Risk Management Reporting Lines* (National Treasury).

[16] *Better Practice Guide - Risk management*, p. 38. June 2008.

failures; escalating new risks and changes in risk profiles to the appropriate level of management in a timely manner; maintaining consolidated risk catalogues; and operating a help-desk function.

*United Nations organizations*

87. The organizations should decide on the appropriate governance structure and degree of dedicated capacity for ERM governance based on an analysis of size, complexity and the nature of their activities, inherent risk profile, degree of sophistication envisaged in risk management, available risk management expertise and the capacity to absorb the additional workload within existing structures.

88. The Inspectors are of the view that United Nations organizations, particularly large organizations with sizeable, distinct departments, diverse field operations, and a profile of significant inherent risk exposure, require a dedicated central risk secretariat/team/officer(s); the establishment of a formal risk committee; and the assignment of a visible leadership/risk champion role to an existing senior executive. The level of sophistication and magnitude of work to be done would justify such governance capacity. In the case of lack of resources, small organizations can choose to assign the risk secretariat/officer function to one or more capable staff as a dual function role.

89. The Inspectors are of the view that, although it is not essential to establish separate formal ERM committees, they are useful and can provide visibility for a formal approach. Where a senior management committee is to handle this function, it needs to be articulated in its terms of reference and risk management should be a standing agenda item.

90. The Inspectors would like to underline that an ERM committee or a senior management committee formally tasked with ERM, are useful, but cannot provide the required managerial leadership. Experience shows that a more effective approach is to assign a corporate risk champion function to an existing senior-level officer. The official in charge of leading ERM should enjoy the necessary authority to direct and coordinate all parts of the organization in terms of risk management. The Executive head should work formally and informally with this official and demonstrate her/his full support.

91. In the light of the differences between large private sector corporations that employ CROs and United Nations organizations, the Inspectors are of the view that there is no need to establish high-level full-time CRO positions in United Nations organizations. However, there is a need for one of the top officials to lead and coordinate the process daily, as corporate risk champion, with recognized responsibility and authority. That said, it should be clear throughout the organization that risk management is an organizational function, not simply an extension of the function of the office/official mandated for coordination and leadership.

92. Although elements of ERM governance exist in United Nations organizations, the leadership position, roles and responsibilities in the implementation process, and reporting and communication lines are not clear, being mainly informal and implicit. Organizations implementing ERM need to formalize leadership and all other roles and responsibilities.

93. In the outcome document of the first risk management exercise, the IMO secretariat identified as one of the lessons learned the need for a strong central coordination function to ensure that the exercise runs smoothly. It further identified that there was a need for the time and

capacity to evaluate risk management results at the corporate level, identify particular areas of concern and plan and monitor the organization’s response to those concerns.[17]

*Location of leadership and secretariat function*

94. ERM is a strategic management issue that covers all parts of an organization; therefore, the leadership and coordination function (corporate risk champion) should be placed at the top. Its location in the organization should make it easy to integrate ERM into strategic planning, programming, RBM and all other operational and business processes. In large organizations, the executive head may delegate this function, preferably to the second in command. The risk champion should be the chairman of the ERM committee and the secretariat risk officer should be placed in his/her office. It is also good practice for the ERM committee to include external member(s)[18] with a good knowledge of risk management, in order to provide an objective and independent view.

*Role of internal audit*

95. The core role of internal audit with respect to risk management is to provide objective assurance on the effectiveness of risk management practices. The Institute of Internal Auditors in its position paper[19] provides three categories for the role of internal audit in ERM: core roles, legitimate roles and roles that internal audit should not undertake. Internal audit departments, depending on their capacity, can play a wide range of roles in the development and implementation of ERM; however, they cannot take the responsibility and accountability for the implementation of risk management, because this is the duty of management. An important function of internal audit is its vigilant attention to ensuring and assessing the identification and management of key risks to the organization. Internal audit departments should take into account risk assessments in the organizations when they prepare risk-based audit planning.

96. In many organizations, internal audit departments play a leading role in the promotion of the ERM concept, including the preparation of ERM documents, workshops and training. Internal audit bodies, with their knowledge and understanding of risk and control theories and concepts, are generally well qualified to assist management in this regard. However, the required safeguards should be in place to ensure that the independence and objectivity of internal audit are maintained, should its involvement in ERM activities go beyond its core roles. In addition, when internal audit is involved in promoting and facilitating the implementation of ERM, there should be a plan that clearly defines at which point the organization’s management will assume full responsibility.

97. In WFP, the oversight division developed the draft ERM policy for approval by the Executive Board and was directly involved in the training of managers in risk management techniques. In UNDP, internal audit promoted ERM and was closely involved until its formal adoption. In FAO, internal audit was a major player in preparing FAO for the introduction of ERM, which is being handled by the Office of Strategy, Planning and Resources Management under the Immediate Plan of Action for FAO Renewal. In UNESCO, internal audit provides the secretariat function to the ERM committee. In UNICEF, internal audit developed a module on risk and control self-assessment, facilitated training and positioned itself to take on a more direct

[17] IMO, Outcome of the secretariat’s first management exercise 2009, document CWGRM 4/2/1.

[18] *Public Sector Risk Management Framework*, p. 49.

[19] Institute of Internal Auditors, *The Role of Internal Audit in Enterprise-wide Risk Management*. Position statement.

role in supporting ERM implementation.[20] So far, no assessment of ERM practices has yet been done by internal audit departments in any United Nations organization, as they have not yet been implemented over sufficient time.

*Role of audit committees*

98. Audit committees have a duty to review the effectiveness of risk management practices and the management of key risks, and report to the governing body. In the United Nations system, in line with the spread of ERM implementation, audit committees increasingly include the review of risk management practices in their agenda. The Inspectors suggest that organizations ensure that the terms of reference of audit committees include risk oversight and that the membership includes those with risk management expertise.

### ***ACABQ report and General Assembly resolution 64/259***

99. The United Nations secretariat, in its recent report entitled "Towards an accountability system in the United Nations system" (A/64/640, para. 78), proposed establishing a dedicated ERM and control function, to be situated in the short term in the Office of the Under-Secretary-General for Management. For the medium term, the report envisages the establishment of a dedicated CRO position with a new independent and objective organizational team. The Advisory Committee on Administrative and Budgetary Questions (ACABQ) did not endorse the proposal of the secretariat as seen below in the excerpt of its report (A/64/683):

> "50. The Advisory Committee emphasizes that risk management needs to be embedded in the various departments rather than in a separate structure, and it should not lead merely to the compilation of a static risk register. The Advisory Committee is not recommending the establishment of the Enterprise Risk Management and Control Section but rather has no objection to a dedicated focus to develop standards, policies and methods and to support managers."

100. The General Assembly, in its resolution 64/259, endorsed the view of ACABQ. The relevant articles of the resolution are as follows:

> "30. *Emphasizes* that the risk management should be dynamic, that it is the inherent responsibility of staff at all levels in the Secretariat, and that each department is accountable for the risk assessment in the delivery of its respective mandate;
>
> "31. *Regrets* the absence of an effective and integrated internal control framework, which is a serious gap in the existing accountability system, and requests the Secretary-General to work on enhancing the current capabilities in the Secretariat responsible for risk assessment and mitigation and internal control, on the basis of the recommendations in paragraphs 49 and 50 of the report of the Advisory Committee on Administrative and Budgetary Questions and annex II to the report of the Secretary-General."

### ***JIU-suggested standards***

101. The Inspectors would like to reiterate that, irrespective of the chosen structure, it is of paramount importance that the governance structure, roles and responsibilities should be clearly defined, integrated into internal policies and procedures, and communicated organization-wide. Based on the review of the literature, best practices, and interviews with officials, the JIU-suggested standards in the division of roles and responsibilities are set out below.

[20] E/ICEF/2010/9, para. 236.

Box 5: Roles and responsibilities in the governance of ERM

| | | |
|---|---|---|
| **Role of oversight bodies** | **Governing body**<br>(a) Ensures that management adopts and maintains an effective risk management process and the appropriate “risk appetite” is set in the organization.<br>(b) Reviews the most significant risks to the organization and management’s response strategies.<br>**Internal audit**<br>(c) Assists in the development and improvement of ERM policies and activities.<br>(d) Assesses the effectiveness of the ERM process and make recommendations for improvement.<br>(e) Ensures and assess the identification and management of key risks in the organization. | **Audit committee**<br>(a) Reviews and advises on the quality and overall effectiveness of risk management procedures and reports to governing body.<br>(b) Monitors the implementation of risk management against implementation strategy/plan.<br>(c) Membership should include risk management expertise. |
| **Role of senior management** | **Executive head**<br>(a) Accountable to the governing body for the implementation of the risk management process.<br>(b) Sets “the tone at the top” and promotes ERM in the organization.<br>(c) Ensures that the overall ERM framework is effective.<br>(d) Makes decisions related to the organization’s risks ensuring that critical risks are known and appropriately managed. | **ERM/senior management committee**<br>(a) Monitors and discusses the overall effectiveness of risk management practices and provides findings to the executive head.<br>(b) Reviews the risk profile of the organization and related action plans.<br>(c) Reviews and evaluates main risk areas and key risks, and determines the overall policy of the organization on how to manage these risks.<br>(d) Monitors and advises on progress in the implementation of the ERM policy and framework.<br>(e) Ensures that key risks are considered in the strategic planning and programming process.<br>(f) Prudent to consider including independent membership. |

| | | |
|---|---|---|
| **Key internal drivers and support structures** | **Corporate risk champion**<br>(a) Works with senior management to develop a risk management policy, framework and strategy.<br>(b) Coordinates the implementation of ERM, and strives to drive it towards best practice.<br>(c) Supports senior executives by coordinating and providing clear and concise risk information that can be used in planning and decision-making.<br>(d) Provides executive support for implementation.<br>(e) Monitors, updates and communicates the organization’s risk profile.<br>(f) Compiles analytical reports for senior management, risk and audit committees.<br>(g) Reports regularly to executive head, risk/senior management committee, and audit committee.<br>(h) Develops and maintains a risk reporting framework for implementation, risk profile, and key risks.<br>(i) Develops and implements an appropriate risk communication and training strategy.<br>**Managers**<br>(a) Responsible for identifying and managing risks related to their unit’s objectives.<br>(b) Ensure appropriate implementation of risk policies and procedures.<br>(c) Define risk management responsibilities in the unit.<br>(d) Ensure that risk management processes are documented.<br>(e) Ensure that risks that cannot be managed at the unit level are escalated.<br>(f) Monitor the risks and risk profiles in their areas of responsibility. | **ERM secretariat/risk officer(s)/team**<br>(a) Assists risk champion and ERM committee and reports to risk champion.<br>(b) Has high-level risk management competency.<br>(c) Assists in the preparation and maintenance of risk management policy documents including guidelines.<br>(d) Helps units across the organization in risk management to ensure a consistent approach is applied.<br>(e) Monitors, consolidates and analyses risk management data for reporting.<br>(f) Assists in the implementation of a training and communication strategy.<br>**Risk focal points**<br>(a) Should have relatively more training and knowledge about risk management.<br>(b) Guide and facilitate the risk management process and advise on use of tools, including risk self assessments, relevant information technology tools, and maintenance of the risk register.<br>(c) Collect and analyse risk data and report to the head of the office and central risk management secretariat.<br>(d) Identify and communicate best practices and lessons learned.<br>**Staff**<br>(a) Support identification and management of risks that affect the achievement of objectives related to the responsibilities of the staff member.<br>(b) Escalate risk issues which are beyond the authority of the staff member.<br>(c) Support the documentation and updating of risk-related information. |

*Benchmark implementation indicator*

102. The Inspectors conclude that in order to implement benchmark 4, executive heads should ensure that there is a formally defined governance structure and clearly established accountability, roles and responsibilities for ERM implementation, including leadership, implementation, monitoring and oversight.

### *Benchmark 5: Communication and training plan to create risk awareness, promote risk policy, and build up general capacity and critical skills for the implementation of ERM*

103. Developing risk management awareness and capability requires the implementation of a well-developed internal communication and training strategy.[21] To manage risks within an organization, a shared understanding of risk management policy and processes is required across all organizational units. The strategy should aim to create awareness, commitment and technical knowledge, as well as facilitate knowledge-sharing throughout the organization. Seminars, workshops, town hall meetings, online training modules and online discussion and knowledge-sharing platforms are useful in this regard. The JIU-suggested elements of the strategy are as follows:

*(a) Develop organization-wide awareness of risk management;*

*(b) Ensure that ERM policy, strategy and processes are understood;*

*(c) Enhance senior management capacity to lead the risk management process;*

*(d) Build up general implementation capacity and risk management skills in the organization;*

*(e) Regularly share and disseminate best practices and lessons learned across the organization.*

104. ERM needs to be approached from the value added perspective, from the point of view of the user. Therefore managers and staff at large need to be involved in the process from the start to ensure buy-in and establish a common understanding. ERM decisions and implementation should not be based solely on the commitment of a few top officials; all managers and staff should share a common conceptual and practical understanding of ERM. Experience indicates that ERM seminars and workshops explaining the concept, benefit and process of risk management targeted at senior-level managers are very useful in creating buy-in at the top level.

105. Training should be tailored in accordance with the existing level of awareness and the level of competency required of each player in the process. It is important that those responsible for coordinating and implementing an organization's risk management plan should have access to detailed competency training. Organizations should use the opportunity to package some ERM training into ongoing training initiatives such as RBM, planning and programming, IPSAS and induction training. It is also best practice that knowledge-sharing mechanisms should be instituted to share best practices and lessons learned.

*United Nations organizations*

106. United Nations organizations do not have documented communication and training plans for the introduction of ERM. However, although ad hoc, there are good examples in the system. UNICEF has provided a number of training and information opportunities through different means, such as a dedicated intranet page, messaging on a social networking site, communities of practice, webinars, regular senior management global broadcast messages, information notes and videos. UNDP has a dedicated ERM webpage, an online ERM course and included ERM as a component in a five-day training course on RBM, as well as in the staff induction training programme. IMO organized a central training course for all focal points, and then the focal points organized individual workshops in their divisions. UNESCO held an organization-wide

[21] *Better Practice Guide – Risk management*, p. 40.

information session and developed a Risk Management Training Handbook[22] and training module. WFP has made its ERM policy and guidance available to all staff on its internal website.

*IFAD and European Commission practices*

107. IFAD released a recorded video message from the President to all staff to promote ERM, and took the training of their divisional focal points one step further by organizing a training course with ERM certification. They organized workshops on cross-organizational issues so that staff could learn from discussions with their colleagues. Officials noted that initially they spent a significant amount of time in their workshops explaining the difference between a risk and a complaint; this was an investment into ensuring proper future risk identification. IFAD officials informed the Inspectors that they also have a webpage and a virtual library of ERM materials that all staff can access at any time.

108. The European Commission holds general risk management courses for managers and key staff; has established a central risk management website; launched specific training for staff responsible for developing risk management skills; and arranged various presentations on risk management for different levels of management. The Commission has also established networks for the exchange of best practices and information. Training courses are available for different levels of the hierarchy (staff, management, Internal Control Coordinators). Specific training can be organized by the Directorates through a framework contract with an external consulting company.

*Benchmark implementation indicator*

109. The Inspectors conclude that in order to implement benchmark 5, executive heads should ensure that there is a documented corporate communication and training plan to promote ERM awareness, establish understanding of risk management processes, develop implementation capacity throughout the organization, and establish knowledge-sharing mechanisms to improve the process.

### *Benchmark 6: Provision of adequate resources to introduce ERM and sustain the implementation process*

*Cost of ERM implementation*

110. Experience shows that in the initial phase of ERM implementation, there is a relatively high need for additional resources; however, this declines over time as the level of implementation increases and more of the work is embedded into core management activities. The Inspectors would like to emphasize that the allocation of both financial and human resources in the context of a plan would increase the success of the project.

111. As seen in annex III, column 2, the cost of ERM varies greatly among United Nations organizations. The cost structure includes direct and indirect costs. Direct costs include the use of consultants, establishment of separate ERM-related positions and structures and purchase of commercial information technology software. Indirect costs include the time spent by existing staff implementing risk management practices, in particular those who lead the process. The United Nations organizations, except UNESCO, have not estimated their indirect costs.

[22] UNESCO Bureau of Strategic Planning, Risk Management Training Handbook, BSP/2009/PI/H/2.

112. Organizations should estimate and look for resources at the planning stage to ensure successful implementation. In particular, a risk management officer/secretariat/team is necessary to support and sustain ERM implementation. Additionally, there is a need for training and seminars to create awareness and build up implementation capacity throughout the organization. Another important element to be considered for successful implementation is to use an information technology solution, which would facilitate easy implementation, and the consolidation, analysis and monitoring of data. Organizations should plan to integrate the necessary modules into existing ERP and other relevant information system platforms, or choose to use special software.

113. According to information received, some organizations have used external consultants at significant cost, whereas others have chosen to implement ERM internally, relying on the existing structure and human resources, with little or no additional cost. Among United Nations organizations, UNDP, UNICEF and UNFPA have a dedicated risk officer for the ERM secretariat function, and only UNDP has special internally developed software.

114. The cost structure can change depending on the size of the organization and degree of sophistication chosen; nevertheless, the cost is not and should not be a decisive factor for the introduction of ERM. Executive heads, when preparing an ERM policy and strategy plan, should estimate the necessary funding to implement it and, if existing resources are insufficient, should ask governing bodies for funding. Governing bodies, in view of the benefits of ERM, should provide the necessary resources. A business case, including a cost-benefit analysis and outline of the policy and plan, would help convince governing bodies to provide the necessary resources.

115. In the case of a lack of resources, executive heads should choose a more simple and gradual approach for ERM implementation, instead of postponing it to the uncertain future. It is a fact that many organizations in the United Nations system have built up significant risk management experience over the years, through individual risk management practices in areas such as project management, business continuity and information systems. They should try to build on this experience to establish ERM as the overarching risk management system.

*Use of consultancy*

116. As seen in column 2 of the table in annex III, some organizations have spent significant amounts on consultants. The United Nations spent $1.32 million for the preparation of the ERM aspect of the first report, A/62/70, in 2008. UNICEF spent $689,711 to undertake the groundwork for the development of ERM policy in 2008. WMO and WHO spent SwF 228,000 and $195,000 respectively on ERM consultancy. It is notable that UNDP and IMO, which are relatively advanced in ERM implementation, did not use external consultancy.

117. In FAO, $2.5 million was estimated and budgeted initially for an externally-driven ERM project. However, an assessment of the organization's approach to risk management concluded that the initial plan, which depended on a large consultancy contract, was unlikely to prove successful or to present an efficient use of limited resources. The new approach called for an internally led project supported by specialized risk management consultants as needed, rather than a consultant-led approach, and the budget allocation was reduced to $1.3 million.

118. It is a major concern for the Inspectors that the use and cost of consultancies varies greatly among organizations, and their value added is not easily identifiable given the absence of a project plan. There is a tendency, in the absence of in-house knowledge, for organizations to outsource issues to consultants with little planning and real engagement. The Inspectors caution that, as long as there is no internal driving of ERM owing to a lack of in-house capacity, consultancy reports are destined to be left, forgotten, on the shelves of archives. Risk

management is the duty of the management and staff of the organizations; therefore, it is essential that there should be internal capacity to drive and sustain the process. Officials in those organizations that are advanced in its implementation stated that ERM should be driven internally for it to be a success. Ownership of the implementation by management has to start from the beginning, with senior management clearly leading the preparation and introduction process.

119. The use of consultancy should be considered in the context of a concrete plan as one of the steps in ERM implementation. Organizations need to develop internal capacity to lead the process and utilize consultants when and if hired. Consultants should always work with these core ERM staff, and most importantly, knowledge transfer from consultant to core staff should be ensured.

*Benchmark implementation indicator*

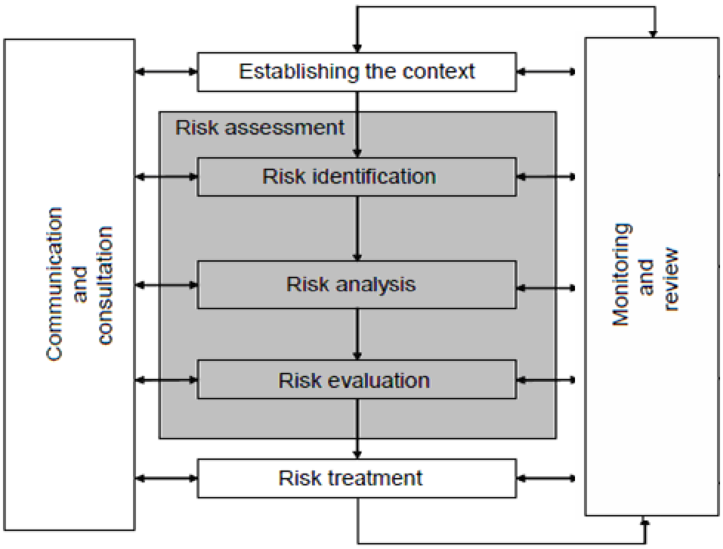
120. The Inspectors conclude that in order to implement benchmark 6, executive heads should prepare the necessary cost estimation together with the ERM project plan, and in the case of a shortage of internal funds, ask Member States for funding. The implementation strategy should be adjusted according to available funding, and where the estimated funding is not immediately available, executive heads should choose a more gradual approach to ERM implementation instead of postponing it.

## *Benchmark 7: Formal risk management process with coherent methodology and tools and clear guidelines for implementation*

*Risk management process*

121. Risk management includes risk assessment (risk identification, analysis, evaluation) and treatment processes.

Figure 1: Risk management process (based on ISO 31000)



122. As an organizational process, ERM requires a coherent methodology and tools to implement it step by step. It has to be formalized and operationalized through a framework, guidelines and other administrative instructions for consistent and correct implementation across organizational units.

### (i) Risk assessment and risk registers

123. Based on the review of the literature and experience, the JIU-suggested criteria for successful risk assessment are set out below:

Box 6: Criteria for successful risk assessment

***JIU criteria:***

*(a) A good and common understanding of the concept of risk;*

*(b) A simple and pragmatic process;*

*(c) A well planned and structured approach with clear goals identified at the outset;*

*(d) A common list of risk areas/risk universe for the organization;*

*(e) An effective internal facilitator to control the process;*

*(f) Clear and adequate guidelines and instructions for implementation;*

*(g) Focus on critical/high risks;*

*(h) Engagement of senior managers and key officials in the process.*

124. Risk assessment includes risk identification, risk analysis and risk evaluation processes.[23] Risk assessment establishes understanding and identification of risks, their causes, consequences and probabilities; and provides a basis from which to determine the most appropriate approaches to respond to risks. Risk assessments should be dynamic, and require regular and continuous updating. Risks are inherent at all levels of an organization and its activities. Therefore, risk assessments can be done at different levels of the organizational structure and operations, such as corporate, departments, divisions, units, processes, programmes, activities and projects.

125. In order to determine priorities for the internal audit activity, risk assessments are also conducted by internal audit, in accordance with the International Standards for the Professional Practice of Internal Auditing. This exercise should not be confused with the identification and assessment of risks for the purpose of ERM. However, an internal audit's risk assessment can be used as an input for ERM, and vice versa.

126. Risk assessments have to be recorded and updated regularly. It is good practice for management to provide standard document templates to support the risk assessment process, including: risk register, incident log, risk assessment, risk escalation, risk profile and risk treatment plan. Electronic templates integrated into the information system would greatly facilitate the consolidation and analysis of the risk data, which is essential for it to be meaningful at the strategic level.

127. Where the organization is small and centralized, with relatively homogenous activities and little delegation of authority, it may choose to have only one risk register. However, if the organization is large, with a considerable field presence and diverse operations entailing more delegation of authority and decentralization, it is important to have multiple levels of risk assessments and risk registers. The risk register does not need to be independent; it can be integrated into planning, programming and RBM platforms. The risk register should not become a static record of risks but a dynamic risk action plan, including significant risks, current controls, time-bound action steps and owners of these actions.

[23] ISO International standard IEC/ISO 31010, Risk management – Risk assessment techniques, p. 12.

128. IMO and UNESCO have only corporate-level risk registers. In UNDP, the units at all levels of the organization (corporate, departmental, regional, and country level) maintain risk logs and update them as often as necessary. IMO, in the context of a pilot ERM exercise, established a risk register and plan to update it with each biennial iteration of the risk management process. In IFAD, divisional, departmental and corporate risk registers are maintained in its corporate results performance system, which is embedded in its information technology system and updated on at least a quarterly basis. Departmental and corporate risk registers are used to capture and manage broader risks affecting the achievement of IFAD's corporate management or strategic objectives.

129. UNICEF risk management policy requires that a risk and control self-assessment must be done on an annual basis at the divisional, regional and country-office level.[24] The risk and control self-assessment is typically facilitated by the risk liaison officers and reported to the respective heads of office, and to the risk management secretariat.

130. In 2006, WFP adopted a corporate risk profile based on the risk assessment outputs of the internal oversight service, and risk registers were established. However, there was a lack of a formal ERM strategy and system to assess, log risks and take mitigating actions. At the operational level, WFP encouraged risk management, especially in more volatile and unstable environments. However, overall treatment of and response to risks were on an ad hoc basis and documentation and consistency were lacking. Risk management remained a recommended practice rather than a mandatory one. This situation, coupled with the lack of a formal governance structure and insufficient resources, resulted in delaying ERM implementation until 2010.

131. In the context of the new corporate performance management framework, WFP is looking at an 18-month time frame for placing on track its ERM framework, and expects ERM implementation to start in the latter half of 2010. Officials explained that they employed consultants to develop the overarching ERM framework; and as of November 2009, a corporate risk profile is in place and is envisaged to be refined based on the completion of the strategic and organizational risk registers.

132. Among other international organizations, OSCE maintains corporate and unit-level risk registers, while the Global Fund has only a corporate-level risk register. The European Commission risk guideline recommends as a minimum establishing an overall risk register at Directorate-General level, but it further suggests that it may also be useful to keep risk registers at directorate and unit levels. It requires risk registers to be updated whenever there is a significant change in the Directorate-General's risk exposure.

*Risk identification*

133. Risk identification is the process of recognition and recording of risks. It entails consolidating and structuring existing knowledge about potential risk events, lessons learned from past experience, "what if?" scenarios, and "horizon scanning" in each area on an ongoing basis. United Nations organizations use workshops, risk self-assessments, surveys, interviews and group discussions to facilitate risk identification. The risk identification process of IMO can be found in annex II of the report.

134. In a number of organizations, electronic voting tools are used for the identification of the important risks among a number of suggested risks. Organizations should choose the techniques

[24] UNICEF, *Enterprise Risk Management Policy*, p. 12.

that are most suited to their needs; however, the same techniques should not be continuously used, in order to avoid making the exercise routine and repetitive.

135. As a lesson learned, some officials stressed that workshops add value by facilitating healthy discussion between different stakeholders; however, a structured approach is required. There has to be a clear agenda, time frame, expected outcomes and a good facilitator. If a consultant is to be used as a facilitator, a knowledgeable officer within the organization should assist and direct discussion towards the specific organizational context.

136. The risk management guidelines should define the basis for the risk management exercise. It is essential that risks are identified in the context of objectives set at each level of the organization, so that risk management helps to achieve the objectives of the organization. From the perspective of United Nations organizations, the RBM initiative can effectively respond to this need. Risks should be identified in the context of objectives and cascading expected results set through RBM.

137. During interviews, the problem was raised that sometimes risk identification and assessment is difficult due to ambiguity in the objectives and expected results. Furthermore formally stated objectives might not help to capture all the relevant dimensions of the risks that face an organization. As a consequence, organizations focus on practical elements, e.g., discussion of organizational objectives, expected benefits, activities and processes, whichever facilitates a meaningful discussion. The Inspectors recognize the value of a flexible approach in risk identification; however, as risk management is done to facilitate the achievement of objectives, organizations should strive to connect risk identification with objectives.

138. Specific, measurable, attainable, relevant, timely (SMART) objectives and expected results would facilitate a healthy risk identification and management process. One of the lessons identified by IMO was that in order to achieve the greatest benefit from applying the risk management process, an improved level of integration with the process for developing and approving the divisional objectives would be beneficial.[25] To that effect, officials consider that risk identification and analysis should be conducted at the time of setting the divisional objectives. The risk identification process of IMO also includes input from Member States.

139. UNICEF’s risk policy document requires that risk should be identified in relation to organizational objectives; and that the risk management secretariat, together with the senior staff/risk committee and directors, conducts an annual review of organization-wide key risk areas.

140. The Inspectors found that the identification of risks in the United Nations system mainly focuses on threats. There is a need to promote and explicitly integrate the identification of opportunities too. In the case of UNIDO, its ERM strategy document is entitled “Risk and opportunity management system”, and provides separate impact scales for opportunity.

*Main risk areas/categories, risk universe and risk profile*

141. A risk universe provides a central repository to define all potential risks and risk events applicable to an organization, regardless of likelihood and impact. It includes an inventory of risks structured under main categories and sub-categories. These ensure the consistent categorization/classification of risks, and also full coverage of all major areas of risk. Thus, it allows for the meaningful consolidation, analysis and monitoring of risks.

[25] CWGRM 4/2/1.

142. The risk profile shows the general status of risk and provides senior management with information on the priorities and management of risks across the organization. It presents an analysis of all risks, including major and newly emerging risks and their areas; a risk map of the organizational structures and locations; and any change in the level of different types of risks. It facilitates the review and monitoring of risk at the strategic level.[26] For instance, it can show that safety and security risks are escalating, or a major financial risk is emerging, or that certain risks in one region are becoming prevalent while declining in other areas. Thus, top management can respond proactively and allocate resources accordingly.

143. The available data on the main risk areas/categories of United Nations organizations can be found in annex III. This shows that the most common risk categories in the United Nations system are operational, strategic and financial. However, there are significant differences between organizations regarding other risk areas/classes. Considering that United Nations organizations have more similarities than differences, it is difficult to justify this much variation with respect to risk categories. This situation is not conducive to having a meaningful United Nations system-wide risk profile and monitoring thereon.

*Top-down and bottom-up approaches*

144. In the identification of corporate risks, organizations exercise a bottom-up (from unit and division levels) or top-down (from senior management level) approach, or a combination of these approaches. Experience shows that a combination of approaches produces better results. In large organizations with diverse activities and a significant field presence, it is important to use a bottom-up approach in combination with a top-down approach. However, risk identification is not confined to these methods. There can also be targeted reviews focused on a few specific activities, particularly for inherently risky areas.

145. The Inspectors would like to emphasize that top-down organization-wide risk identification should not be underestimated and ignored. Indeed, it is vital for ERM that it provides an organization-wide, top-down view. While each individual unit of an organization can identify risks from their point of view, top management, taking into consideration the identified risks from all parts of the organization, would have the advantage of seeing and assessing risks from the perspective of the whole organization. In the case of a top-down approach alone, it would be doomed to failure, as it would not reflect the findings of people at the forefront of the organization's operations.

146. In UNDP, corporate risks are identified through three main processes: (i) escalation from country offices and other units through the online risk system; (ii) interviews with bureau directors; and (iii) analysis by the ERM secretariat. The ERM committee reviews and decides on the corporate risks and their treatments. In IFAD, both bottom-up and top-down approaches to risk identification are used. Key risks are elevated to a higher level and a filtering process is used to identify top risks (first voting tool, then consensus).

147. A bottom-up approach was used to arrive at a risk register for the WMO secretariat. Risk workshops were conducted for major departments and also separately for General Service staff. During workshops in the first session, participants identified risks facing their department and the secretariat as a whole, and voted to rank their impact, and the vulnerability of WMO to these

[26] United Kingdom, *The Orange Book: Management of Risk - Principles and Concepts* (Norwich, HM Treasury, 2004), p. 20.

risks. In the second session, treatment strategies (including risk owner, action plans and time frames) for top-ranking risks were developed by the participants.[27]

148. The Global Fund follows a dual approach for assessing and prioritizing risk: a strategic level review (top-down) and an operational level review[28]. During the most recent risk identification exercise, teams were encouraged to get together and agree on risks; then unit directors went off-site to review and agree on them and add more if they felt that it was required. Afterwards, in a top-level retreat, these risks were validated and prioritized, including the addition of new risks.

149. In one of the directorates (Directorate-General for Maritime Affairs and Fisheries) of the European Commission in which the Inspectors had an interview, risk identification is performed in the context of 22 key business processes and the activities they involve. Officials explained that, where business processes are cross-departmental, risk identification workshops are organized which include key staff from all departments concerned. This facilitates the dialogue between risk owners and leads to the effective identification of risks and hence the strengthening of internal controls.

*Inherent risk versus residual risk*

150. Risks can be identified and assessed on an inherent and residual basis. A risk without consideration of any controls is defined as an inherent risk. A risk after the consideration of controls is defined as a residual risk. Thinking about risk often focuses on residual risks, since this shows the actual exposure of the organization. There is a tendency in United Nations organizations to use only one step to directly identify residual risks, although they are not clearly named as residual risks. The argument is that it is not the risk professionals who assess the risks, but rather managers and staff who intuitively think about residual risks.

151. Organizations have to choose their preferred method based on the phase and degree of sophistication of ERM implementation. At its simplest, only residual risk identification would be useful in the early stages of learning and adoption of risk management; however, the Inspectors suggest that, as implementation matures, organizations should move to identifying both inherent and residual risks, in order to make the process more useful and meaningful. Relying only on residual risk identification might result in losing potentially useful information on the risk events that the organization is facing, and make the process too simple to benefit from. Particularly in the area of internal controls and process-related risks, it is invaluable to identify and document inherent risks, control procedures and residual risks as a basis towards establishing a sound internal control system in the organization.

152. The European Commission identifies and documents inherent risks, existing controls, and finally, residual risks. OSCE identifies and documents inherent risks; assesses and documents current risk, based on documenting the existing controls in place; and assesses their operational effectiveness by performing walk-through tests for each control. Finally, the OSCE assesses and documents controlled risks taking into account the effectiveness of proposed controls that are planned for future development.

[27] WMO Internal Oversight Office, annual accountability report, document EC-LXII/Rep.7.2(6), appendix B, p. 9.

[28] The Global Fund to Fight AIDS, Tuberculosis and Malaria, *Risk Management Framework* (2009), para. 3.12.

### (ii) Risk analysis, evaluation and treatment

153. Risk analysis and evaluation include three scales of measurement – *impact*, *likelihood* and *risk level* (see the figure below). The following formula illustrates the relationship of these scales: *Risk level = Impact x Probability*. Risk analyses are done by estimating both the likelihood of the risk, and the impact if the risk occurs. Based on the analysis of impact and probability, a risk evaluation has to be done for each risk to determine the significance/level of risk.

154. Impact, probability and risk level should have defined categories to be used in the assessment, e.g., low, medium and high. No standards exist for the quantity and names of categories. However, it is important that whatever categories are used, they have to be applied across the whole organization so that risk assessments are consistent and comparable, and allow meaningful aggregation and analysis.

155. As seen in column 3 of annex III, in the assessment of probability and impact of risks United Nations organizations mainly use three or five categories, which result in 3 x 3 or 5 x 5 risk matrices. For instance, the categories low, medium and high can be presented as a 3 x 3 risk matrix. Only ILO uses two categories, low and high. For the risk evaluation, too, organizations use similar or different number and name of categories.

156. Organizations determine the categories which best fit their circumstances; however, the Inspectors are of the view that the use of more categories is better for classification and prioritization and, ultimately, a more detailed and meaningful evaluation of results. Having fewer categories inevitably leads to a high concentration of risks placed in one category, which might require further refining and prioritization.

157. Risk analysis methods can be quantitative, semi-quantitative or qualitative, depending on the subject area, application and data availability. With any of these methods, the issue is to determine the level of impact of a risk if it occurs, and the level of likelihood of its occurrence. For instance, while the impact of a major information technology system failure can be estimated as *significant* (anticipating that it would interrupt critical business processes for more than a few days), its *likelihood/probability* could be calculated, taking into account existing control measures and available failure statistics in departments, as statistically less than 5 per cent.

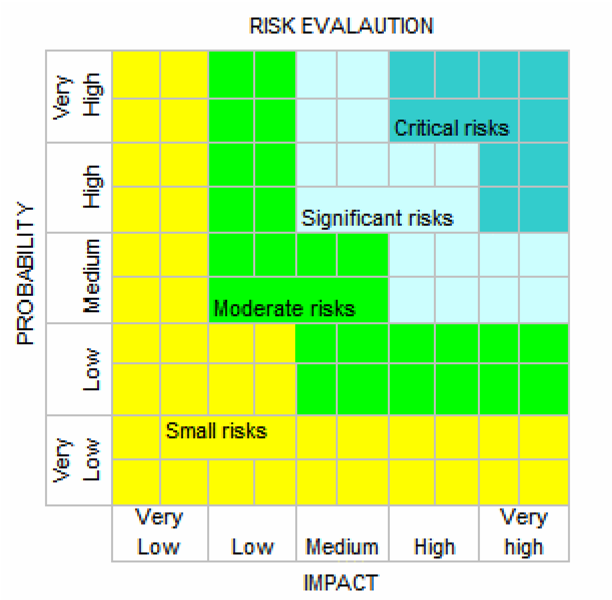
158. United Nations organizations at the moment rely mainly on available experience and best judgement, rather than statistical data. Quantitative techniques require reliable statistics, hence reliable information systems. Since qualitative assessments involve a degree of judgment, it is necessary to document assumptions and validate the results, for instance, using brainstorming sessions with the involvement of different levels of staff.

159. Based on the result of risk analysis, a risk evaluation has to be undertaken to reach a decision regarding the significance/level of each risk to the organization and whether it should be accepted or treated. It provides the ranking of risks in terms of priority for the organization. It is important that organizations define risk-level categories and develop criteria to evaluate the significance of risks, including the boundaries for tolerance/acceptance, in order to facilitate decisions for treatment. It was noticed that, in some organizations, a sum of money is used as the criteria for establishing the significance of financial risks, while for risks that can cause disruption to operations, the length of disruption is used.

*Risk matrix*

160. For an easy illustration of risk analysis and the evaluation process, a risk matrix exhibiting impact, likelihood and risk level is shown below:

Figure 2: Risk analysis and evaluation matrix



161. As seen above, risk evaluation categories are established on the risk matrix as small, moderate, significant and critical. The sum or intersection of impact and probability scores will automatically fall into one of these categories and risks are thus prioritized so that decisions can be taken on their treatment.

162. Once risks have been analysed, evaluated and prioritized, organizations need to determine the appropriate responses for each risk. In broad terms, response options can include: tolerate/accept, treat/reduce, transfer and avoid. The level of acceptable risk is known as the "tolerance level" and provides the benchmark for an organization's risk tolerance. It can be defined according to the significance/rating of risks. For instance, in the matrix above, while small and moderate risks can be considered tolerable, critical and significant risks would not be acceptable and critical risks would have priority for treatment. The costs and benefits of risk treatment have to be considered for each decision. In deciding whether a risk is acceptable or not and its treatment, the expected benefits from the actions associated with the risk would be taken into account. Risk treatment actions should be time-bound and recorded. To ensure that risks are treated, risk owners must be identified and held accountable for taking the necessary actions according to the treatment plan.

163. In general, the use of risk assessment scales is not well-developed in United Nations organizations. The use of assessment categories for impact, likelihood and risk evaluation is fairly immature. To some degree, this is to be expected given that ERM implementation is at an early stage in the organizations. There are also ambiguities in the definition and use of categories and practical implementation methods. The lack of clear guidelines exacerbates the situation.

*IMO experience*

164. IMO uses three categories in its risk evaluation, i.e., low, significant and severe. In the first iteration of IMO's risk management process, 79 risk events were identified. According to the risk evaluation conducted, these risks were categorized as follows:[29] 6 per cent low, 89 per cent significant and 5 per cent severe. The concentration of almost all risks in the higher risk categories is not conducive to risk management, as risks so classified would require treatment and would therefore be in competition for limited resources.

165. The IMO secretariat identified as a problem the lack of differentiation between degrees of risk, rendering analysis less straightforward. Because of the lack of detail in the risk analysis and evaluation categories and definitions, most risk events were scored as "significant". The practical implication of this was that the majority of the risk events identified were assessed as being outside the tolerance level and requiring further treatment, which did not necessarily reflect the feeling of those who conducted the exercise. Large numbers of staff requested further guidance on the approach to be applied in determining risk tolerance. The IMO secretariat provided additional detail for the numerical scoring of the risk for each risk event and is considering introducing a fourth risk category to allow a greater degree of focus on the most significant risks.

*Risk appetite and risk tolerance*

166. In any decision regarding risk acceptance and treatment, the organization's risk appetite and risk tolerance level plays a role. Risk appetite is the overall amount of risk judged acceptable for an organization, while risk tolerance is the level of variation the organization is willing to accept around specific objectives. The setting of the risk appetite for an organization is complicated. It is determined based on the existing risk profile, risk capacity and risk tolerance. Risk tolerance is determined, in practice, according to the interpretation of defined risk evaluation categories in each risk assessment.

167. As ERM implementation is increasingly absorbed into the corporate culture and the level of sophistication increases, organizations may benefit from describing their risk appetite within each of their main categories of risk, such as financial, operational, and reputational. Organizations should try to aggregate risk management results in each major area and consolidate them at corporate level, with a view to ensuring that the organization's risks are appropriate, balanced and sustainable.

### (iii) Focusing risk management

*Focus on top corporate risks*

168. It is the duty of top management to devote time and attention to the identification, management and monitoring of key corporate risks. The number of corporate risks should be manageable, and only include important risks whose management would provide the most value added to the organization. A group of top risks from the corporate risk registers of UNDP, IMO and UNESCO are included in annex I.

169. In UNESCO, 31 risks were identified at the senior managers' retreat. Afterwards, they were rated against each of the 56 objectives via an online survey, and ultimately 10 were identified as top corporate risks. One of the risks identified was that there is no succession planning, although 30 per cent of the staff would retire in the next three to five years. This risk was discussed in the

[29] CWGRM 4/2/1, p. 4.

Risk Management Committee and it was sent to the human resources department as the identified owner of the risk.

170. The UNDP corporate risk log includes 12 risks. In IFAD, the identification of risk was first done through cluster workshops using a bottom-up approach. The ERM committee reviewed these risks, streamlined them to 14, and presented them to the management committee.[30] Using a voting tool, the management committee finally selected five top risks, identified the risk owners and set out mitigation strategies.

*Focus on limited number of important risks*

171. Good risk management focuses on high probability risks that may have a major impact on the achievement of objectives. Organizational units with little or no experience in ERM might have a tendency to formally identify and document all possible risks, resulting in an overwhelming number of risks, which would not be easy to manage. To avoid this problem, each organizational unit, at least at the beginning of the ERM process, should focus on a limited number of important risks. As experience is gained, the number of risks to be registered and treated could be expanded to include other risks. The focus on high impact and high probability risks should not lead organizations to ignore other risks. Low probability but high impact risks should in particular be monitored, as they may materialize in the future.

172. The European Commission risk management guideline suggests singling out and focusing on critical risks in order to make risk management effective and keep documentation and reporting down to a reasonable volume. The Directorates-General, however, are encouraged to identify and monitor other significant risks that require follow-up. In one Directorate-General, officials explained that they suggest that divisions register the most important five risks and, in any event, not more than 10.

173. In the United Nations organizations, there is no explicit policy or instruction in this area. UNDP officials explained that, in the first risk assessment exercise, roughly 10 risks were identified in country offices. Thereafter, staff were strongly encouraged to focus on five critical risks. The new UNDP unit work planning guidance suggests that risk assessment in the work plan should focus on a few major risks that the unit plans to take action on, and/or monitor, during the work plan period.

*Cross-cutting risks and risk escalation*

174. Cross-cutting risks often require action by more than one organizational unit and the identification and treatment of cross-cutting risks is one of the most important features of ERM, which benefits from having an integrated and organization-wide approach. In particular, key corporate risks are often cross-cutting in nature in terms of both their impact and the necessity to take action at many levels for mitigation. Cross-cutting risks require the involvement of different departments and all related parties should be identified and recorded, and the risk assigned to the most suitable manager to coordinate and lead the risk response.

175. United Nations organizations in general lack guidelines for the identification, treatment and escalation of cross-cutting risks. Only UNDP has escalation procedures. The head of the unit is responsible for escalating a risk and escalation is done through the existing management chain. The Inspectors found that the European Commission had detailed instructions with respect to cross-cutting risks between its services.

[30] IFAD, annual report on ERM activities in IFAD, document EB 2010/99/R.30, para. 11.

### (iv) Information technology tools: commercial software, open source software and ERP

176. In the United Nations system, no organization uses commercial software for ERM. Officials expressed the view that commercial software was not readily adaptable for United Nations organizations, as their risk universe and processes were private-sector-oriented. UNDP uses internally developed software for documenting risk assessments and responses. An intranet portal for managing unit and corporate risk logs has been made available and is being used by 88 per cent of units. Other organizations use simple spreadsheet and Word-based templates to register and follow-up on risks.

177. WFP officials explained that, with a large number of staff and a widespread country presence, ERM cannot be implemented without information technology support. It should be a service that the organization is providing to staff for easy and effective implementation, without creating a serious additional burden. Therefore, they are considering using a special software platform that will automatically process a wealth of information, allow for dashboards and reporting, and be compatible with the existing WFP information system.

178. IFAD integrated some modules into its existing ERP system to facilitate ERM implementation. OSCE uses commercial software, which was purchased for 50,000 euros and the license and maintenance cost is 15,000 euros annually. The software allows all staff to see all identified risks and controls, time-bound actions, and the current status of implementation across the organizational units.

179. IMO officials, after the first risk assessment exercise, identified as a lesson learned the need for a simple system or database to record, report and analyse results; a mere list of the completed risk event tables does not provide a user-friendly means of assessing and reporting on the data gathered. The development of a simple tool, which would allow querying by category and classification by range of criteria, would simplify and streamline the process of reviewing the data, and allow patterns and areas of concern to be more easily identified.[31]

180. Experience shows that the use of special software enables organizations to reap more benefits from ERM including better analysis and monitoring opportunities. Organizations, particularly large organizations, should try to develop an information technology solution such as the development or purchase of special software, or if possible the integration of modules into existing systems, e.g., ERP and RBM platforms, in order to better operationalize ERM. However, special software is not a precondition to start ERM implementation. The Inspectors note that there is open source software available for risk management, e.g., free open source software is being used for risk management in a major ERP project in the United Nations Secretariat.

### *Need for clear methodology and guidelines*

181. The Inspectors would like to reiterate that ERM implementation requires a formal risk management process with a coherent methodology and tools. Organizations have to formally establish impact, likelihood and risk-level scales and relevant categories, escalation procedures and the practical steps to be taken to implement all these processes. There is a need for clear guidelines with adequate detail, including the description and interpretation of risk categories and their application in practice. Furthermore, organizations need to establish mechanisms for feedback and lessons learned, in order to use experience to improve the process. Adequately detailed guidelines coupled with continuous coaching and regular iterations would help to refine the process.

[31] CWGRM 4/2/1, p. 6.

*Benchmark implementation indicator*

182. The Inspectors conclude that, in order to implement benchmark 7, executive heads should ensure that a formal risk management process is established with coherent methods and tools, and clear guidelines and instructions, easily accessible to all staff, with a view to ensuring the consistent and integrated implementation of ERM throughout the organization.

### *Benchmark 8: Integration of risk management with RBM, planning, programming, and operational and business processes*

183. Risk management is not, and should not be, a stand-alone exercise or a separate administrative structure. Risk management might become a simple compliance exercise rather than an effective management tool if it is not integrated with the major processes of the organization. Integration would provide purpose in applying the risk management processes and relate risk back to the organization's objectives and core activities; it would also ensure that the task of managing risk is not regarded as an additional responsibility or burden, but part and parcel of all processes. Integration should also include the harmonization of individual risk management practices under an overarching ERM framework in order to ensure consistency in approach and support more efficient use of resources. As a natural extension of integration, risk management should be mandatory and embedded into the performance management process. This would enhance accountability, help to create a risk aware culture and speed up implementation.

184. ERM practice requires risk management in all areas, including ongoing operations and processes, as well as one-off initiatives, such as information technology projects, capital master plans, corporate strategies and policies and field projects. Risk assessment should be part of the decision-making process; one measure to promote this is to require risk assessments to be attached to all important policy, strategy and project proposals presented to the senior management committee.

*Experience in United Nations organizations*

185. The experience of UNDP sheds light on the challenges and solutions for successful ERM implementation. One year after the introduction of ERM in UNDP, the ERM committee requested a stocktaking exercise. Based on the results, the committee concluded that, although improvements were evident, the management of risk was often ad hoc and reactive, took place as a stand-alone exercise and that practices varied within offices and across the organization.[32]

186. UNDP recognized that risk management was not yet fully integrated with organizational processes and that this would be the main challenge going forward. As a first step, unit-level risk logs are being streamlined and integrated into organizational work planning as a means to tie risk management to overall RBM and to support dialogue between individual units and their oversight units on the combined opportunities and challenges related to results and risks. Responses to major risks will be included as key results with associated activities in the unit's work plan. Officials informed the Inspectors that they are reviewing all policies, plans, strategies and operations to ensure that risk management is appropriately integrated into all areas.

187. IMO is working to integrate risk identification with the identification of objectives. FAO officials informed the Inspectors that in the preparation of the programme of work and budget for 2010–2011, they integrated risk identification in relation to strategic objectives. One of the IFAD corporate management results is improved risk management. Through the divisional management

[32] UNDP, Framework for Risk Management in UNDP, discussion note, February 2010.

plan, divisions can identify, assess and then define appropriate actions to mitigate or exploit risks that may constrain or enhance their ability to achieve planned results. The preparation of divisional plans requires risk identification and quarterly performance reporting, which is mandatory for all divisions as part of the strategic planning and reporting process.

188. WFP officials explained that the reasons for the creation of the new Performance and Accountability Division are to bring together results-based and risk-based management; to provide support to the ERM committee; and, most importantly, to build a better bridge between the risk management activities at the country-office level, and the corporate oversight of those risks and their mitigation. The Division created a corporate performance management framework, dubbed the "wheel for performance", to support the implementation of the 2008–2013 strategic plan, which establishes a holistic view for performance management. The framework integrates risk management and internal control elements. Officials further explained that if ERM were introduced as part of performance management, its value added would be recognized, because it would be related to the work of each staff member.

189. In order for an organization's risk management systems to be considered as ERM, they also need to cover one-off initiatives. In the United Nations organizations there is no systematic coverage yet in this regard. Some of the major reform initiatives, such as organizational restructuring, business process change and offshoring, lack a proper risk management process, while some other major initiatives, such as ERP and the capital master plan, include risk management. For instance, risk management has been applied throughout the life of a major ERP project and the capital master plan in the United Nations. Officials informed the Inspectors that the capital master plan has a risk register that is reviewed and updated several times a year under the coordination of a risk manager. Each risk is assigned a colour code based on an assessment of the likelihood of the risk and its impact on the project. Each individual risk is monitored by a risk owner, who also makes a risk assessment, develops a risk mitigation strategy, sets a trigger point and develops a risk response.

*European Commission experience*

190. One of the key principles of risk management in the European Commission is to embed risk management into existing planning and decision-making processes. The standing instruction for annual management plans requires that each department's plan has to identify the main risks which may have an impact on the achievement of objectives, and take appropriate actions to address them. In addition, risk management is explicitly integrated into the Commission's internal control framework.

*Risk management in dependencies, partnership and humanitarian assistance*

191. In many cases, organizations' risks are connected with the risks of third parties. The risks of major contractors usually become the organization's risks. For instance, if major business processes were outsourced, the risks of the contracted company would become the risks of the organization. Another fact is that the success of some United Nations organizations increasingly depends on implementation partners in the field. The achievement of programmatic objectives increasingly depends on events that are partially or fully beyond the control of the organizations, and which must be managed in cooperation with partners and other stakeholders. This situation requires organizations to approach risk management involving all partners systematically.

192. Risk management can be used effectively in the preparation of programmes related to development operations and humanitarian aid, based on risk assessment in the regions. Another important area to consider using integrated risk management is the delivery of emergency aid in natural disaster-stricken areas, to ensure fast and effective aid delivery by all parties.

193. These issues are yet to be integrated formally into the ERM policy and practices of the United Nations organizations. Organizations should develop modalities and protocols, integrate them into ERM policy and frameworks and provide guidelines for their practical implementation.

*Integration into RBM*

194. Both ERM and RBM have overlapping aims of achieving the objectives of the organizations. While RBM sets objectives at each level and directs the work of the organization towards achieving them, ERM aids this process by enabling staff to identify, assess and manage risks related to achieving those objectives. Many United Nations organizations have embarked on implementing RBM. Given that RBM has to cover all parts of an organization including planning, programming, budgeting and operations, the Inspectors are of the view that it is a unique opportunity for the organizations to integrate ERM through RBM processes.

*Integration with internal control systems*

195. As a broader concept, ERM incorporates internal controls as an integral part of risk management. ERM brings strategic objectives into play within an overarching risk management framework[33] and supports that internal control system is being assessed and established towards achieving strategic objectives of the organization.

196. The European Commission uses risk management to reinforce sound internal control systems. Internal control coordinators usually coordinate the risk management practices in each Directorate-General. Directors General are required to make a declaration on the overall state of internal controls in their annual reports.

197. In United Nations organizations, ERM is not explicitly linked to internal control systems. In view of the close relationship between effective risk management and sound internal control systems, executive heads of United Nations organizations should utilize ERM to improve internal controls and speed up the establishment of a sound internal control framework as a major element of ERM.

*Assessment*

198. The Inspectors note that the integration of ERM into planning, programming, business and operational processes, performance management and one-off initiatives is yet to be done in United Nations system organizations. However, officials are generally aware that integration is lacking and plans are being made to rectify this. It would be more efficient if organizations considered integrating ERM into existing organizational processes and new initiatives at the planning stage. While pioneer organizations expedite the integration process, other organizations should consider integration in the planning stages based on the experience and lessons learned already available. Organizations, taking this opportunity, should also consider establishing a sound internal control system as an integral part of ERM.

*Benchmark implementation indicator*

199. The Inspectors conclude that, in order to implement benchmark 8, executive heads should ensure that ERM is integrated into RBM, planning, programming, operational and business processes, as well as one-off initiatives and humanitarian assistance activities. In addition, dependency and partnership risks should be included in risk assessments.

[33] *Enterprise Risk Management – Integrated Framework*, appendix – Relations between ERM framework and internal control integrated framework.

### *Benchmark 9: Monitoring, evaluation and reporting mechanisms to ensure compliance with, and effectiveness of, risk management*

200. The risk management cycle is not complete without the establishment of monitoring, review, evaluation and reporting processes. Effective and fully established risk management frameworks incorporate mechanisms for this purpose, both formal and informal.[34] Both performance and compliance aspects of risk management should be reviewed and reported. The JIU-suggested elements for these processes are set out below:

Box 7: Elements of monitoring, evaluation and reporting

***JIU suggested elements:***

*(a) The progress of the overall ERM implementation plan*

*(b) Assessment of overall performance/effectiveness of risk management*

*(c) Compliance with risk management policy, framework and guidelines*

*(d) Monitoring and reporting risk management at each level*

*(e) Risk profile of the organization, emerging critical risks and their management*

*(f) Periodic review and update of the risk management policy and framework*

*(g) Internal and external reporting mechanisms*

201. The communication, monitoring and reporting of local risk management practices follow existing management lines, and are the duty of respective managers in their sphere of work. Risk management is one of the key responsibilities of all staff, and can be effective only through a formalized process including the integration of risk management duties and actions into performance assessments. It should be part of management performance at every level.

202. Overall performance, effectiveness and compliance reviews are the responsibility of top management, the risk champion, and risk/senior management committees. The internal audit department has to make an objective assessment of the overall adequacy and effectiveness of the risk management process. Other oversight functions, such as external audit, inspection, investigation, evaluation, and policy review, within their professional line of duty and expertise, also have a role to play in objectively assessing the functioning of the risk management mechanisms.

203. The main institutional oversight actors for overall implementation include, internally, the ERM and senior management committees, and externally, the finance committee, audit committee, and governing body. The finance committee reviews risk management in the area of its mandate. While senior management has a duty to ensure effective risk management in the organization, the audit committee assists the governing body to fulfil its oversight role.

204. Monitoring and review can be effective only through the establishment of corresponding reporting mechanisms. External risk reporting to the audit committee and governing body can be

[34] *Better Practice Guide – Risk Management*, p. 30.

done separately, or in conjunction with RBM and planning and programming documents. Internal reporting would include formal and informal communication and reporting channels. Reporting to the ERM/senior management committee, audit committee and governing body need to be formalized.

*Experience in United Nations organizations*

205. In UNDP, the ERM Committee meets on a quarterly basis to review the overall effectiveness of risk management, and analyse and prioritize the main corporate risks, including actions to be taken. Units are encouraged to implement risk monitoring within their regular processes for the monitoring of work plans. Externally, reporting to the Executive Board on the implementation of risk management is performed as an integral part of reporting regarding the progress of implementing the Strategic Plan.

206. UNDP officials informed the Inspectors that, during the first two years of implementation, they were tracking risk log completion in all units across the organization. Given that targets were reached, they are now working to develop enhanced indicators that will track the extent to which risk assessments are updated and action taken to respond to risk. The aim is to move towards more quality-oriented monitoring. Officials further explained that the Audit Committee has specific responsibilities to exercise oversight on risk management and internal control systems.

207. IMO envisages that, at the completion of each biennial iteration of the risk management process, a summary report would be sent to the senior management committee, and to the Council through the intergovernmental working group, setting out key areas of risk, mitigating measures, responsibilities and timescales. IMO also plan to conduct a review across the organization to identify lessons learned and produce periodic reports for the senior management committee or the Council, as appropriate, covering changes and actions. In UNICEF, a summary report, including the organization-wide risk profile and risk matrix that provide a summary view of the key risks facing the organization, is planned to be submitted to the executive office.

208. In IFAD the ERM committee reviews and monitors the ERM process and outputs on a regular basis. Monitoring of ERM-related actions is carried out as part of the quarterly performance reviews which are conducted as part of each divisions' annual work plan. The audit committee and the Executive Board are reported to on an annual basis. The audit committee periodically conducts a review of the risk and risk management procedures of IFAD, and reports to the Executive Board on the outcome of such reviews.

*European Commission experience*

209. In the European Commission, in general, internal control coordinators within the individual Directorates-General act as risk management facilitators and monitor the implementation of action plans. Risks are reviewed whenever it is necessary within the directorates. Directorates General are requested to report critical risks and corresponding mitigating actions in their annual management plans and implementation results in annual activity reports. The annual activity report provides an overview of critical risks encountered and their impact on the achievement of the objectives. A synthesis report, which provides a condensed overview of the annual activity reports, is provided to the Council, the European Parliament and the European Court of Auditors.

***Oversight role of the governing body***

210. Governing bodies of the organizations are responsible for setting policies, providing direction and exercising an oversight role on implementation. Therefore ERM project and policy papers should be submitted to the governing bodies for their information, guidance, oversight and request for additional funding if needed.

211. In view of the importance of having an effective risk management process, and the strategic implications of critical risks, it is imperative that governing bodies should exercise their oversight role. Clear direction and continuous oversight by governing bodies are essential to ensure the success of ERM initiative. Often the mitigation of critical risk would require the decision and support of governing bodies. As main stakeholders, Member States must be kept abreast of the status of ERM implementation and the strategic and emerging critical risks that an organization is facing. There should be regular reporting to governing bodies regarding the status of ERM implementation and the identification, treatment and monitoring of critical risks in relation to the strategic objectives of the organization.

*Assessment*

212. Overall in United Nations organizations, the monitoring, review, evaluation and reporting of ERM are yet to be clearly formulated, formally established and properly implemented. Internal reporting channels exist; however, these are mostly informal, implicit and not regularly used. External reporting to and oversight on the part of governing bodies are generally lacking, with the possible exception of IMO. In the case of IMO, there is close oversight by, and involvement of, the governing body with the preparation of the ERM policy and framework, as well as with the implementation process. Due to the early stage of ERM implementation, no internal audit or external evaluations have yet been undertaken.

*Benchmark implementation indicator*

213. The Inspectors conclude that, in order to implement benchmark 9, executive heads should ensure that: ERM monitoring and evaluation mechanisms with corresponding roles and responsibilities are established and communicated across the organization; and that there is periodic and structured internal and external reporting to all relevant stakeholders, regarding ERM implementation and the management of key risks. Additionally, the Inspectors would like to emphasize that governing bodies should exercise their oversight role regarding the implementation of ERM, and review and discuss emerging critical risks and response strategies.

### *Benchmark 10: Inter-agency cooperation and coordination, including the development of a common ERM framework, knowledge-sharing mechanisms, and management of common and cross-cutting key organizational risks*

214. Over the years attempts have been made towards improving inter-agency knowledge sharing across the United Nations system. In 2007 and 2008, UNDP coordinated a network of ERM practitioners across United Nations organizations. In December 2009, the United Nations Secretariat hosted a two-day inter-agency meeting on accountability and ERM. A good example of inter-agency cooperation took place in 2008, when the High-level Committee on Management (HLCM) of the United Nations System Chief Executives Board for Coordination (CEB) set up a steering committee for staff safety and security to prepare recommendations and options for a more effective United Nations system-wide security management system, including risk management. The steering committee recommendations were endorsed by HLCM and received strong support from CEB.[35]

215. Another example is a sub-working group of the inter-agency standing committee on emergency preparedness, which is leading inter-agency efforts to institutionalize preparedness in

[35] See document CEB/2009/HLCM/INF.1.

humanitarian country teams through the timely use of contingency planning, early warning systems and scenario simulations. A harmonized emergency risk management initiative has been piloted in four countries, which aims to streamline various risk-based planning processes into regular office planning.[36]

216. Further cooperation opportunities have been suggested by some organizations. UNICEF has a community of practice which has been mentioned as a useful source of practical information; its officials expressed their willingness to share with other organizations. WFP is considering using the UNDP e-learning module on risk management.

*Assessment*

217. Interviews confirmed that there are some good examples of knowledge and experience-sharing regarding ERM practices in the United Nations system; however they are largely ad hoc and unsystematic. There are no formal or informal networks, platforms or mechanisms to facilitate this process. No system-wide cross-cutting, common or critical risk identification attempts have been made. Existing policy and frameworks diverge greatly in terms of terminology, methods and approaches. There is no joint risk management process developed for joint or complementary programmes and country operations.

218. Organizations should consider establishing formal or informal networks and platforms under HLCM to facilitate knowledge sharing, including internet or intranet platforms. While initially an informal network would be useful, as ERM practices spread across the system, a formal network would be more appropriate.

219. The Inspectors found that a number of organizations are trying to develop their own stand-alone policies and frameworks, often through the use of consultancy firms, without utilizing existing documents or tapping into the experience and capacity of other United Nations organizations.

220. The Inspectors are of the view that many organizations that are about to embark on ERM can develop their policy and strategy by drawing on existing inter-agency knowledge, expertise and experience, rather than outsourcing to a consultancy firm. Instead of going through the same process of trial and error, the organizations with the advantage of not being pioneers in ERM implementation should make an effort to benefit from the experience, documents and capacity of the pioneer organizations.

221. The United Nations system – through the CEB – should consider developing a common ERM policy and framework with sufficient flexibility to be used by all organizations. It would greatly help in harmonizing practices, saving costs, and facilitating the establishment of a system-wide risk universe and risk profile, which would enable organizations to develop joint and more effective and efficient risk response strategies. It would also provide a common risk management language throughout the system.

222. The Inspectors would like to draw attention to a common policy and framework used by all Directorates-General of the European Commission. The overall framework[37] establishes a general framework to facilitate consistent implementation and provides flexibility for each Directorate-General to develop procedures most suitable to their specific circumstances.

[36] E/ICEF/2010/9, para. 173.

[37] European Commission, Towards an effective and coherent risk management in the Commission services, document SEC(2005)1327.

*Common, interrelated and cross-cutting risks*

223. The Inspectors are of the view that a significant number of corporate-level risks might be common to the majority, if not all, of the United Nations organizations. In addition, the management of some critical risks in one organization might affect risks in some other organizations. Many risks are likely to be common, particularly at the country level, where organizations operate in parallel; also, it might be the case that different risks are interrelated.

224. There are also cross-cutting risks which would benefit from a consolidated or integrated response from all organizations, such as reputation, safety and security. In addition, given the fact that United Nations organizations are striving to deliver as one, organizations should consider exercising combined risk assessments and risk registers at the country level, by country teams, with a view to responding to risks effectively with a common strategy and action plan.

225. In view of the existence of system-wide common and interrelated critical risks, it would be very useful to include the review of these risks as a regular agenda item of CEB. The Inspectors are of the view that if a common risk universe were compiled for the United Nations system organizations, such a common repository could be beneficial for harmonizing risk management practices, as well as for establishing and monitoring a system-wide United Nations risk profile.

*Benchmark implementation indicator*

226. The Inspectors conclude that for the implementation of benchmark 10, the executive heads through CEB should:

- Establish a formal or informal ERM network. Such a network could facilitate the systematic sharing of risk management experience and lessons learned;
- In parallel to the maturity of ERM practices in the system, include the review of a system-wide risk profile, and key common and cross-cutting risks, into its regular agenda items;
- Discuss and initiate the development of a common ERM policy and framework for all United Nations organizations, with a view to harmonizing practices, establishing a common risk universe and developing a system-wide risk profile.

Additionally, executive heads should:

- Consider adopting an inter-agency integrated risk management approach wherever possible, particularly at the country level, and develop modalities to that effect.

## IV. CONCLUSION AND RECOMMENDATIONS

227. The report provides nine benchmarks for the successful implementation of ERM in each organization. The review of organizations’ practices shows that, except for the first benchmark (adoption of a formal ERM policy and framework), most of the organizations are not yet at a stage to satisfactorily fulfil the remaining eight benchmarks. As pioneers, only UNDP and IMO can be considered close to fulfilling some other benchmarks, particularly the commitment and engagement of executive management, and communication and training. A few organizations have not yet considered ERM. Other organizations are either preparing policies, or have just adopted policies and are moving on to pilot exercises. Overall, United Nations organizations can be considered as beginners regarding ERM implementation.

228. ERM adoption and integration into the organizational culture is slow in the United Nations system. There are many reasons for this, such as a lack of collective understanding and commitment by senior management; lack of a formal implementation plan; uncertainty about how to implement and integrate ERM into organizational processes; lack of an appropriate governance structure; and the pressure of competing reform initiatives. In addition, the fact that ERM is a relatively new management tool and is still evolving means that organizations do not have a clear road map to follow.

229. Benchmark 10 is related to system-wide coordination and cooperation and requires joint action by all organizations. It is clear that, while it is necessary to adjust the ERM approach according to the specific nature of each organization, there is a need for a system-wide approach so as to ensure the speaking of a common language within the system on ERM; the identification and management of key common and cross-cutting risks (e.g. safety and security and reputational risks); avoidance of duplication; and optimal use of scarce resources.

230. The 10 best practice benchmarks identified in the report form a solid framework to be followed by the organizations. The Inspectors believe that if United Nations organizations were to follow the benchmarks as best practices and tenets for the effective implementation of ERM, in addition to reflecting the best practices available, and sharing information, lessons and expertise from within the system, the organizations could make rapid headway towards developing appropriate ERM use and application. This must be accompanied with the full support of governing bodies and senior management.

231. In view of the benefits of full ERM implementation, the Inspectors suggest that, in the light of the analysis and recommendations of this report, the executive heads of the United Nations system organizations should take stock of the existing situation and speed up ERM implementation.

*The Recommendations*

232. The Inspectors are of the view that the first nine benchmarks laid out above should be adopted and implemented as a package by each executive head to ensure successful ERM implementation in their respective organizations. Benchmark 10, which requires inter-agency cooperation and decisions, should be discussed and adopted at the level of CEB. As the Chairman of CEB, the Secretary-General of the United Nations should pursue the implementation of the recommendation addressed to CEB.

233. The implementation of recommendations 1 and 2 below is expected to enhance the effectiveness of the organizations. Recommendation 3 is expected to enhance coordination and cooperation among the organizations.

**Recommendation 1**

**Executive heads should adopt the first nine benchmarks set out in this report, with a view to ensuring that the ERM approach is accepted and implemented in line with best practices.**

**Recommendation 2**

**Governing bodies should exercise their oversight role regarding the adoption of ERM benchmarks set out in this report, the effectiveness of implementation and the management of critical risks in their respective organizations.**

**Recommendation 3**

**The CEB through the High-level Committee on Management (HLCM) should adopt benchmark 10 of this report with a view to facilitating inter-agency cooperation, coordination, knowledge sharing, and the management of common and cross-cutting risks, for more effective and efficient risk management throughout the system.**

## Annex I
## A group of top risks (and risk areas) from UNDP, IMO and UNESCO

UNDP

1. The changing aid architecture, environment of economic crisis and urgency with regards to climate change represents a significant opportunity to (re)position United Nations and UNDP as a valued partner (strategic)
2. Volatility of key currencies and fluctuating capital markets (financial)
3. IPSAS implementation (financial)
4. Implications of contractual reform in UNDP (organizational)
5. Staff safety/security in the face of urgent and real threats to United Nations system and increasing costs related to security (operational)

IMO

1. Financial system failure and loss of back-up data (operational)
2. Lack of buy-in and cooperation from key staff for the implementation of results-based budgeting (operational)
3. Financial failure of major provider/supplier (operational)
4. Delays and breakdowns in processing access of delegates to meetings and in the registration of delegates (operational)
5. Unforeseeable unavailability of interpreters owing to circumstances of force majeure (operational)

UNESCO

1. Lack of a succession plan may leave UNESCO with a significant gap in terms of competent senior staff, given the anticipated retirement of Professional staff over the coming biennium (staffing)
2. Inability to articulate, to achieve, and to report on quality results may lead to a loss of confidence in the ability of UNESCO to deliver, a loss of visibility and eventually a reduction in funding (RBM, quality of programme delivery and visibility)
3. An imbalance in influence and decision-making processes between central services and the programme sectors may impact on programme delivery and quality (organizational design and accountability)

## Annex II
## Risk identification process in IMO

✓ Senior management workshop to establish the purpose of the risk event identification and to identify significant top-level risks;

✓ A self-assessment exercise for key operational staff within each division, to identify risk events within their area of operation;

✓ Follow-up interviews with key staff by a central risk team designed to validate the results and detect gaps in identification, in particular through the use of “what if …?” analysis;

✓ Seek the input of all stakeholders through a review of the risk event identification by Committees and Sub-Committees;

✓ The continued role of the Council Risk Review, Management and Reporting Working Group as a forum to provide input from the Member States into the risk management process and, in particular, with regard to risks relating to organizational status and effectiveness. This might involve: identification of scenarios for “what if …?” analysis; review and commentary on such analysis; identification of specific risk events.

Source: IMO risk management framework.

## Annex III
## Overview of ERM in the organizations of the United Nations system, and European Commission, OSCE and the Global Fund

| Organization | ERM status<br>(1) | Cost of implementation<br>(2) | Impact, probability and evaluation scales<br>(3) | Main risk areas<br>(4) |
|---|---|---|---|---|
| United Nations | In the planning stages of ERM.<br>An ERM and internal control framework is being developed. Phased approach is planned to be used. | $1.32 million spent on the consultancy for the enterprise risk management aspect of the first report of the Secretary-General on accountability framework, ERM and internal control framework, and results-based management framework.[38] | Ref. A/64/640.<br>*Impact:* 1. Low; 2. Moderate; 3. High; 4. Significant; 5. Critical<br>Probability: 1. Low; 2. Moderate; 3. High; 4. Significant; 5. Critical<br>Control effectiveness: 1. Highly ineffective; 2. Ineffective; 3. Significant improvement needed; 4. Limited improvement needed; 5. Effective<br>Risk evaluation scales;<br>Tier 1, the most significant risks requiring high-level attention;<br>Tier 2, moderate risks requiring specific remedial or monitoring measures;<br>Tier 3, risks expected to have low risk exposure and a low residual risk. | The risk universe includes a catalogue of 116 risks in five major risk areas: strategic, governance, operational, compliance and financial. |
| UNODC | Not yet considered. | - | - | - |
| UNEP | Not yet considered. | - | - | - |
| UN-HABITAT | Not yet considered. | - | - | - |
| UNHCR | Not yet considered. | - | - | - |
| UNRWA | At the beginning of ERM.<br>In 2009, the draft concept of risk registers was tested in the Agency, and in 2010, it is planned to have risk registers completed for all offices.<br>For the beginning, offices are expected to focus on the top dozen risks. This process is expected to take the biennium 2010–2011 to complete. | An external facilitator was contracted to support ERM implementation process. | Impact and likelihood scales; high, medium or low. | N/A |

[38] ACABQ report A/63/457, page 8, Para 25.

| Organization | ERM status<br><br>(1) | Cost of implementation<br><br>(2) | Impact, probability and evaluation scales<br>(3) | Main risk areas<br><br>(4) |
|---|---|---|---|---|
| | Advisory Committee suggested a risk officer be placed in the executive office. However due to resource constraints UNRWA is planning to appoint a part time focal point for risk management in the executive office. | | | |
| UNDP | The ERM policy came into effect in 2008. An enhanced ERM framework was endorsed in 2010.<br>The first stage of ERM implementation completed in 2008. It was introduced at both corporate and unit level.<br>Efforts to strengthen ERM continued in 2009 and 2010–2011 biennium.<br>ERM Secretariat, comprising of one, full time, P-4 position. The software used for documenting risk assessments is integrated with unit work-planning. | Internal resources used. There was also pro bono work by a consultant. | *Impact* is assessed from the point of development results, programme and operations, safety and security, reputation and trust, financial impact, time for recovery, and the scope.<br>*Impact*: 1. Negligible; 2. Minor; 3. Moderate; 4. Severe; 5. Critical<br>*Probability*: 1. Very unlikely; 2. Unlikely; 3. Moderately likely; 4. Likely; 5. Very likely<br>Depending on risk level, a decision to accept risk can be made by different level of management line. | Strategic<br>Environmental<br>Financial<br>Organizational<br>Operational<br>Political<br>Regulatory |
| UNFPA | In the planning stage of ERM. A Senior Risk Advisor position, at P-5 level, has been placed in the Change Management and Business Continuity Office (part of the Executive Office). The governance architecture will be put in place as part of ERM strategy in 2010. | External consultancy (approximately $75,000) was used to assist the development of an ERM strategy. | N/A | N/A |
| UNICEF | At the beginning of ERM. There is an ERM policy and framework (2009). It is envisaged to be implemented with organizational improvement reforms, which is planned to be completed by 2012.<br>Chief, Risk Management, P-5 position, was established in the Change Management Office. | External consultancy was hired to undertake the ground work for the development of the ERM Policy and related tools in 2008. Total cost is $689,711.59 ($600, 000 for fee and $89, 711.59 for travel and misc. expenses) | *Impact* is assessed in terms of its effect on the achievement of programme objectives, reputation, personnel and financial.<br>*Impact*: 1 negligible; 3 moderate; 5 critical.<br>*Likelihood*: 1 unlikely; 3 likely; 5 certain.<br>*Risk significance/evaluation*: low, medium to low, medium to high, high. | 26 key risk areas have been identified which are grouped in four categories: Financial, Hazard, Operational, Programmatic/Strategic. |

| Organization | ERM status<br>(1) | Cost of implementation<br>(2) | Impact, probability and evaluation scales<br>(3) | Main risk areas<br>(4) |
|---|---|---|---|---|
| WFP | In planning stages of ERM. First ERM policy was introduced in 2005 but not implemented. As of 2009–2010, an ERM framework is being developed and it is expected that it will be implemented within 18 months starting in the later part of 2010.<br>Phased approach is adopted. Country offices will volunteer to be pilots. | $3.1 million is available for 2010/11 for strengthening performance and accountability including ERM. External consultants are contracted to assist in the development of the ERM framework. | *Impact*: 1. Low, 2. Medium, 3. High<br>*Probability*: 1. Low, 2. Medium, 3. High<br>*Risk evaluation/Seriousness*, based on average score of: 1 to 3 low, 3 to 6 medium, 6 to 9 high<br>(they are being reviewed) | External environment<br>Reputation<br>Funding<br>Organizational capacity<br>Staff motivation and flexibility<br>Security<br>(they are being reviewed) |
| ILO | At the beginning of ERM.<br>ERM policy was announced in 2009. Headquarters offices will be trained by the end of 2011 and external offices' training will begin in 2011. | Funds for training of staff are estimated at $400,000. Plans to hire a consulting firm to provide training based on the training materials internally developed. | High and low are used for both assessing the *impact* and *probability*. Category medium is intentionally avoided so as to eliminate an opportunity to avoid making critical decisions. | Physical security,<br>Financial, Programme and execution ,<br>Reputation,<br>Political |
| FAO | At the beginning of ERM. Plans to implement ERM in 2010-2011.<br>There is no policy document yet.<br>Pilot based approach will be used and ERM will be introduced along with RBM. | FAO first envisaged an external consultant driven ERM and reserved $2.5 million dollars for this purpose. Later, it was decided to have an internally driven project. Thus, Programme of Work and Budget 2010-2011 allocated $1.3m funding. | N/A | N/A |
| UNESCO | At the beginning of ERM. As of 2008, ERM is gradually being implemented under the supervision of the Risk Management Committee.<br>New senior management is in place since 2010. ERM implementation is on hold until the transition period of the new management is over. | A consultant was hired to develop the training module. The undertaking of the risk-based evaluation of UNESCO's capacity to deliver and the set-up of the Risk Management Committee is estimated at a cost of one man year of staff time; however, this cost was absorbed by the staffing structure in the Internal Oversight Service. The maintenance of the Committee and all related communication are estimated at a cost of approximately half a man year; however, these staff costs have also been absorbed by the existing staffing structure of the services involved in ERM. | *Impact*: Significant, Moderate, Minor<br>*Probability*: Low, Medium and High.<br><br>Risk evaluation/seriousness rating is the multiplication of the impact and likelihood where;<br><br>Low = avg. score 1-3<br>Medium =avg. score > 3-6<br>High = avg. score > 6-9 | Resourcing programmes,<br>Governance,<br>Staffing,<br>Organizational design and accountability,<br>Financial management,<br>RBM,<br>Quality of programme delivery and visibility,<br>Delivering within the United Nations system,<br>Director General's mandate,<br>Africa,<br>Priority Gender Equality |

| Organization | ERM status<br>(1) | Cost of implementation<br>(2) | Impact, probability and evaluation scales<br>(3) | Main risk areas<br>(4) |
|---|---|---|---|---|
| ICAO | In planning stage of ERM.<br>Policy is to be developed in 2010.<br>Implementation planned for 2011. | Funds allocated for start up of ERM amount to CAN $25,000 for external consultancy support. Other anticipated costs are CAN $48,000 ($3,000 for seminar, $15,000 for project plan, $20,000 for pilot project, $10,000 for evaluation, update and roll-out). | N/A | N/A |
| WHO | At the beginning of ERM. Started implementation in one cluster.<br>The ERM concept and framework will be expanded to entire Organization in future, however no fixed time frame has been determined yet. | US $195,000 was spent for the support of external consultants. | N/A | Financial<br>Organizational<br>Operational<br>External agents and stakeholder |
| UPU | ERM planning is scheduled for 2010.<br>In June 2010 UPU Conducted a risks assessment exercise assisted by an external consultancy company. The main findings will serve as a basis for the formulation of an ERM policy. | The cost of external consultancy was around SwF 18,000. | N/A | N/A |
| ITU | Discussing ERM | N/A | *Impact* and *probability* categories are measured on a scale of three levels; low, medium and high. | Governance<br>Strategic<br>Resources<br>Operational |
| WMO | At the beginning of ERM. Risk assessments and departmental risk registers were developed in 2009.<br>A comprehensive ERM will be embarked upon due when funds become available.<br>There is a risk management framework, but no policy as yet.<br>A Strategic Planning and Risk Management Officer, P-5 level, was appointed in the strategic planning office in 2009. | Two external consulting firms were hired in 2006 and 2008 to introduce and facilitate ERM process in two phases. Total cost of contracts is SwF 228,000. There was no budget provision; activities were funded from High Priority Reserve. | *Impact* and *probability* categories used are on the scale of 1. Low to 4. High. | Strategic<br>Operational<br>Financial<br>Governance |

| Organization | ERM status<br>(1) | Cost of implementation<br>(2) | Impact, probability and evaluation scales<br>(3) | Main risk areas<br>(4) |
|---|---|---|---|---|
| IMO | In the first stage of full-scale implementation as of 2009, after completion of a pilot exercise.<br>Risk Management Framework exists since 2008. | To date no specific direct costs have been incurred in the implementation of ERM. The existing staff perform additional functions. | Training documents define impact categories in monetary terms, and in terms of its information, political and occupational, and health and safety impact.<br>*Impac*t: 1. Very Low; 2. Low; 3. Medium; 4. High; 5. Very High.<br>*Likelihood* is expressed as the percentage chance of occurring in time frame.<br>*Likelihood*: 1. Rare; 2. Unlikely; 3. Moderate; 4. Likely; 5. Almost Certain.<br>*Risk* is evaluated based on the score (impact + likelihood): < 4 Low<br>4 to 8 Significant, > 8 Severe | Organizational status and effectiveness<br>Financial<br>Operational |
| WIPO | Considering | - | - | - |
| UNIDO | At the beginning of ERM. The first phase in 2009 mainly focused on training on risk awareness and risk identification for senior management. An ERM policy will be finalized as part of the ERM strategy, which will be formulated during 2010. | External consultants were used to develop methodology and facilitate workshops.<br>The cost was €30,000. | *Impact of a risk*: 1. Minor; 2. Small; 3. Moderate; 4. Considerable; 5. Critical; 6. Disastrous<br>*Impact of an opportunity*: 1. Minor; 2. Small; 3. Moderate; 4. Large; 5. Very Large; 6. Extreme<br>Each category is associated with a monetary amount of loss/gain compared to the baseline.<br>*Likelihood*, whether risk or opportunity: 1. Unlikely; 2. Seldom; 3. Possible; 4. Likely; 5. Almost Certain; 6. Certain. | Leading processes<br>Core processes<br>Supporting processes<br>External influences |
| UNWTO | Not yet considered | - | - | - |

| Organization | ERM status<br>(1) | Cost of implementation<br>(2) | Impact, probability and evaluation scales<br>(3) | Main risk areas<br>(4) |
|---|---|---|---|---|
| IAEA | At the beginning of ERM.<br>Has a formal framework. Beginning of the planning process.<br>PROBIS software is used for ERM purposes. | Initial spending on consultants for the development of the policy and to conduct the training workshops was US $30,000. Programme and budget information system expenditure for the development and implementation of Risk Register is €5,000. | N/A | Organization has not decided on categories of risks, however, the ultimate risk is reputational risk. |
| IFAD | Implemented since 2008 when the policy and ERM committee were established. The work-plan for 2010 includes finalization of ERM framework documents, training and communication activities, finalization of the corporate risk profile and register.<br>Training courses provided: a workshop on ERM, training of ERM focal points, project risk management training, ERM intranet site containing ERM tools and library. Some modules are integrated into Peoplesoft. | ERM is being implemented largely within the existing structures. The total additional expenditures for external consultancy services, publications and the voting tools amounted to approximately US $150,000 during 2008/2009. It is expected that the continued maintenance of ERM would cost approximately US $50,000 per annum. | *Impact*: 1. Negligible, 2. Low, 3. Moderate, 4. Significant, 5. Major, 6. Catastrophic.<br><br>*Probability*: 1. Virtually impossible, 2. Unlikely, without precedent, 3. Unlikely, but not unprecedented, 4. Likely to occur, 5. Highly likely, 6. Virtually certain to occur. | Resource planning and management,<br>Country programme,<br>Financial,<br>International policy,<br>Advocacy,<br>Business continuity |
| European Commission | ERM policy and framework document exist since 2005.<br>A pilot exercise was carried out in 2004/2005. Implementation activities from 2005 to 2007 included: introducing risk management in the Annual Management Planning process; developing Risk Management Guide; developing an optional generic questionnaire for risk identification and assessment. | Initial investment comprised mainly of training provided to all levels of staff and the reallocation of internal resources, in particular the installation of Internal Control Coordinators in every Directorate-General/service.<br>The total cost of external consultancy in the area of risk management training (development and implementation) amount to €258,000 since 2005.<br>The five service contracts that covered the full process of the introduction of the risk management framework (pilots, development of methodology, development of the framework, drafting the communication, implementation guide, facilitation of implementation) amount to around | Suggests two options to Directorates-General for *impact* and *likelihood*: low, medium or high, or 1 to 5 scales. The most commonly used ranking is low, medium, high. | External environment<br>Planning, processes, and systems<br>People and the organization<br>Legality and regularity aspects<br>Communication and information |

| Organization | ERM status<br>(1) | Cost of implementation<br>(2) | Impact, probability and evaluation scales<br>(3) | Main risk areas<br>(4) |
|---|---|---|---|---|
| | | €890,000. However real use is less than full amount, since services were requested and provided by the contractor as "flexible" assistance to central financial service team which was in charge of the development of the risk management framework. | | |
| The Global Fund | The risk management framework and policy were introduced in September 2009. | At the beginning, consultants were used to understand the process, but implementation was led internally. | Risks are assessed from impact, significance and probability point of view as low, medium, or high. | Strategic<br>Operational<br>Portfolio risks |
| OSCE | The rolling out of ERM on the administration side is already underway and subsequently will roll out to programmatic side.<br>Guidance document exists.<br>Training workshops were structured as half a day of theory and half a day of risk and internal control identification.<br>Commercial software is used as a repository of all risk-related information. | External consultants were used for 10 workshops and training for the cost of approximately €50,000.<br>The software was purchased for approximately €50,000 and additional €15,000/year will be spent for its maintenance. | *Impac*t: Critical, High, Medium, Low, Very Low<br>*Probability:* Near Certainty, Highly Likely, Likely, Not Likely, Remote<br>*Risk evaluation*: High, Medium, Low | External<br>Strategic<br>Reputation<br>Financial<br>People<br>Technology<br>Security<br>Legal |

## Annex IV
## Overview of action to be taken by participating organizations on JIU recommendations
## JIU/REP/2010/4

| | | | | United Nations, its funds and programmes | | | | | | | | | | | Specialized agencies and IAEA | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **Intended impact** | **CEB** | **United Nations*** | **UNCTAD** | **UNODC** | **UNEP** | **UN-HABITAT** | **UNHCR** | **UNRWA** | **UNDP** | **UNFPA** | **UNICEF** | **WFP** | **ILO** | **FAO** | **UNESCO** | **ICAO** | **WHO** | **UPU** | **ITU** | **WMO** | **IMO** | **WIPO** | **UNIDO** | **UNWTO** | **IAEA** |
| **Report** | **For action** | | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| | **For information** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **Recommendation 1** | | **e** | ▨ | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E |
| **Recommendation 2** | | **e** | ▨ | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | L | ▨ | L | L | L | L |
| **Recommendation 3** | | **c** | E | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ |

| **Legend:** | | |
|---|---|---|
| | **L:** | Recommendation for decision by legislative organ |
| | **E:** | Recommendation for action by executive head (*in the case of CEB by the Chair of the CEB) |
| | ▨ | Recommendation does not require action by this organization |

**Intended impact: a:** Enhanced accountability **b:** Dissemination of best practices **c:** Enhanced coordination and cooperation **d:** Enhanced controls and compliance **e:** Enhanced effectiveness **f:** Significant financial savings **g:** Enhanced efficiency **o:** Other

* Covers all entities listed in ST/SGB/2002/11 other than UNCTAD, UNODC, UNEP, UN-Habitat, UNHCR, UNRWA.