UNITED NATIONS DEVELOPMENT PROGRAMME
Office of Audit and Investigations

Empowered lives.
Resilient nations.

AUDIT

OF

UNDP ENTERPRISE RISK MANAGEMENT SYSTEM

Report No. 1181

Issue Date: 4 April 2014

Table of Contents

Report on the audit of UNDP Enterprise Risk Management System
Executive Summary

The UNDP Office of Audit and Investigations (OAI) conducted an audit of the UNDP Enterprise Risk Management (ERM) system from 10 June to 2 August 2013. The audit assessed the adequacy of UNDP's ERM policy and practices at all levels of the organization (Headquarters, Country Office and project levels) as they relate to the quality and usage of risk management tools and reports. The audit did not cover the assessment of the adequacy or reasonableness and impact of management actions in managing various risks at UNDP.

OAI viewed the adequacy of UNDP's ERM policy and practices from two angles: First, OAI assessed the extent of compliance by comparing the ERM practices with existing ERM policies and procedures. Second, OAI identified areas for improvement by comparing these ERM policies and practices against internationally recognized standards on risk management, best practices of other organizations and benchmarking studies.

At the corporate level, OAI assessed the ERM function exercised by the Bureau of Management (as the secretariat of the ERM Committee) and ERM Committee (merged within the Organizational Performance Group since 2011). At the operational level, OAI reviewed a sample of 4 Headquarters bureaux, 5 Country Offices, and 18 development projects, which were all selected based on specific criteria, such as the size of offices, project expenditure level, different risk types as defined in UNDP's risk management policy, geographical range, and experience from past audits.

The audit covered the relevant ERM activities during the period from 1 January 2011 to 30 June 2013**.** While adequacy of the risk management system is generally covered in all of OAI audits, this was the first audit of the ERM system per se since the ERM policy was approved in 2007.

The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

Overall audit rating

OAI assessed the UNDP ERM system as **unsatisfactory**, which means "internal controls, governance and risk management processes were either not established or not functioning well. The issues were such that the achievement of the overall objectives of the audited entity could be seriously compromised." This rating was mainly due to inadequate implementation of the ERM cycle at various levels of the organization and the breadth of improvements in policy, tools and practices that are needed when compared with internationally recognized standards, good practices of other organizations, and benchmarking studies relating to ERM.

OAI noted that risk management activities take place in UNDP, in different realms, involving different actors and levels of the organization, and oftentimes on an ad-hoc and informal basis. OAI noted, however, that oftentimes risk management activities were not channeled through the ERM structures, procedures and systems.

OAI also recognized that the implementation of ERM can be a challenging and transformative endeavor, particularly given UNDP's decentralized business model and the widespread geographical presence. In such contexts, successful implementation of ERM calls for sustained improvements and adjustments before it could be effectively integrated across all activities of the organization.

In Country Offices and Headquarters bureaux, there was in general, limited appreciation of the existing formal corporate ERM mechanisms as business units generally did not see the value-added/benefit of reporting risks and ERM was not sufficiently integrated in the actual decision-making process of the organization.

OAI recognized that this point was addressed in the Operation Support Group handover note of September 2011 to the Bureau of Management, in which it provided lessons learned on ERM implementation since its introduction in UNDP in 2007. The note states that the main challenge for ERM "rests with its proactive use as it is still perceived as a stand-alone, and not linked to actual decision-making", including resource allocation and support.

Key recommendations: Total = **3,** high priority = **2**

For high priority (critical) recommendations, prompt action is required to ensure that UNDP is not exposed to high risks. Failure to take action could result in major negative consequences for UNDP. All high (critical) priority recommendations are presented below:

Weaknesses in the risk management cycle at corporate and operational levels (Issue 1)	At the corporate level, there were infrequent reviews and updates of the corporate risk log. At the operational level, while risk identification was mostly carried out in a systematic manner, there was limited evidence of follow-up and review of initial risk logs, including the implementation of mitigating actions and an assessment of residual risks. Overall, the quality of information recorded in risk logs at the operational level was low. This creates the risk that critical risks are not evaluated, responded to, monitored, and/or escalated to the appropriate levels. <u>Recommendation</u>: Follow-up on the implementation of, and strengthen the reporting on the five steps of the risk management cycle (identification; assessment; prioritization; taking action; and monitoring and reporting) at all levels of the organization.
Weaknesses in existing ERM policy and practices (Issue 4)	OAI noted a range of weaknesses in the existing ERM policy and practices when compared to internationally recognized standards of risk management and good practices, particularly on the following principles: (a) definition of roles, responsibilities and resources; (b) integration of ERM with existing management and decision-making processes; (c) usefulness and user-friendliness of systems, tools and guidance; and (d) critical mass of knowledge and understanding of ERM procedures and requirements. <u>Recommendation</u>: Building on lessons learned from the ERM implementation since 2007, and considering best practices on risk management, redesign the ERM policy, procedures, tools and practices, as appropriate, and identify the level of resources that would be necessary for a successful organization-wide update and sustainability of ERM.

Management comments and action plan

The Director of the Bureau of Management accepted all the recommendations and is in the process of implementing them. Comments and/or additional information provided have been incorporated in the report, where appropriate.

Issues with less significance (not included in this report) have been discussed directly with management and actions have been initiated to address them.

Helge S. Osttveiten
Director
Office of Audit and Investigations

I. The ERM system in UNDP

The concept of ERM in UNDP was introduced by OAI (then the Office of Audit and Performance Review). An external firm, contracted by OAI, drafted an ERM model and presented its approach at the UNDP Global Management Team Meeting in January 2006, where an initial risk assessment was actually done. Thereafter, an ERM working group was formed and the ERM policy was approved on 23 February 2007. The policy was later integrated into the Programme and Operations Policies and Procedures.

The UNDP Accountability Framework, which was approved by the Executive Board in September 2008, includes ERM as one of its essential elements. The Framework states that "at all levels of the organization, risks are identified, risk profiles are maintained, and management responses are prepared and monitored as an integral part of UNDP operations. Enterprise risk management thus has a direct impact on all other elements of the accountability framework."

At the corporate level, there were two main bodies tasked with ERM responsibilities: First was the ERM Committee which managed the more strategic risks. This Committee was tasked with ensuring that the overall ERM framework was effective and relevant and being applied UNDP-wide and with making decisions related to corporate risks, including which risks were priorities and what actions were to be taken to manage the risks. The ERM Committee was an independent body until 2011, when the decision was taken to include the ERM Committee into the Organizational Performance Group, since the two groups had a common membership.

Second, and in parallel to the ERM Committee and the Organizational Performance Group's subsequent assumption of the ERM functions, UNDP also established a more operational risk management mechanism on the corporate level, namely the Executive Team, which served to address risks and problems in high risk Country Offices that required immediate attention and action by senior management. The Executive Team was headed by the Associate Administrator or the Director, Bureau for Crisis Prevention and Recovery, and the Directors of all relevant corporate bureaux and offices as well as Resident Representatives or their delegates.

The ERM policy was originally developed under the auspices of the Operation Support Group. This office supported ERM until the end of 2011 when the secretariat function was transferred to the Bureau of Management. In the Bureau of Management, a management specialist was responsible for Business Continuity Management and ERM. This post served as the Secretariat to the ERM Committee, and was intended to ensure that ERM is conducted, that actions to address risks are implemented, that risk data is analysed to identify trends and patterns in risks across the organization, that the risk profile is presented to the Organizational Performance Group and relevant bureaux, that relevant policies are updated, and ERM materials and tools are further developed.

II. Detailed assessment

A. Compliance with UNDP policies and requirements

1. Risk management cycle at corporate and operational levels

OAI reviewed the ERM cycle, which is defined by the following five steps: (a) risk identification; (b) assessment; (c) prioritization; (d) taking action; and (e) monitoring and reporting. The review covered the corporate and the operational levels.

Issue 1 Weaknesses in the risk management cycle at corporate and operational levels

According to the Programme and Operations Policies and Procedures, the activities to be carried out by staff at the various levels of the organization for each of the five steps of the ERM cycle shall "ensure that ERM remains a continuous, proactive, and integrated process throughout UNDP."

At the corporate level:

OAI reviewed the existing corporate risk log and compared it with the earliest version available, which was dated January 2012 and noted that the information recorded hardly changed between then and September 2013. The risk log did not show significant changes of risk exposures as an effect of mitigating actions taken or changing mitigation strategies.

Further, OAI noted infrequent meetings regarding risk management on a corporate level. The ERM Committee originally planned to meet quarterly, and subsequently decided to reduce the frequency of its meetings to semiannually. At the time of the audit fieldwork in August 2013, ERM had only been discussed twice since early 2011. OAI concluded that the ERM cycle at the corporate level did not seem to follow a formalized process and may not have been functioning effectively.

At operational levels:

The five-step cycle for ERM as described in the Programme and Operations Policies and Procedures stipulates that reporting on risks is performed at all levels of the organization as part of the implementation of the unit work plan. This should include reporting on progress, problems, timelines, results, outcomes, change made or recommendations implemented.

OAI noted that there was mostly a process for risk identification at the operational level, e.g. at the onset of a project or in the context of preparing unit work plans. However, OAI found limited reporting on follow-up on risk status, effectiveness of mitigating actions, and residual risks. Further, such limited documentation was found only in 4 out of 18 projects and in 1 out of 9 bureaux and offices that were sampled.

Weaknesses in reporting of the steps taken subsequent to the risk identification in the five ERM cycle steps as well as infrequent review and updating of the corporate risk log may lead to critical risks not being evaluated, responded to, and/or monitored at the appropriate time.

Priority High (Critical)

Recommendation 1:

Follow up on the implementation of, and strengthen the reporting on the five steps of the risk management cycle (identification, assessment, prioritization, taking action, and monitoring and reporting) at all levels of the organization.

Responsible HQ bureau: Bureau of Management

Management action plan:

In response to the draft report, while management agreed with the need to better formalize the process and to update records, management indicated that there was no evidence that this led to any mismanagement of risk. Management further commented that, at the corporate level, evidence showed that risks have been re-evaluated/validated even when no changes to the corporate risk log were made. Also, when risks were still relevant, no change to the risk log was expected or needed. Management indicated that while formal ERM discussions occurred infrequently, there was ample evidence that risks, recognizing their severity and likelihood, and mitigation strategies were discussed in the Organizational Performance Group without necessarily calling it an ERM session. Management concluded that many of the decisions and policies approved by the Organizational Performance Group explicitly reference risks contained in the corporate risk log.

Nonetheless, management agreed to take the following actions:

(a) Update the corporate risk log and ensure the ERM Committee meets to discuss risks on a regular basis.
(b) Introduce risk management as part of project quality assurance.

Estimated completion date: December 2014

OAI Response:

OAI appreciates the actions taken by management and will review evidence of action taken as part of OAI's follow-up process.

2. Communication channels

Issue 2 Inadequacies and insufficient use of ERM communication channels

According to the Programme and Operations Policies and Procedures, "communication regarding risks follows regular reporting lines and should, generally, be done through the Enhanced Results Based Management platform to ensure that accountabilities are clear and documented." OAI reviewed a sample of the ERM-related communication mechanisms at all levels of the organization, projects, Country Offices, Regional Bureaux, other Headquarters units/bureaux and the ERM Committee/Secretariat and concluded that communication of risks was often not carried out through established/formal communication mechanisms, in particular using the "risk tabs" of the Integrated Work Plan. All interviewees from Country Offices stated that major risks and issues were communicated to Headquarters through alternative communication channels e.g., email or telephone, and thus not captured in the risk log. This was also reflected in the handover note of the Operations Support Group to the Bureau of Management.

Further, it was noted that even when using formal mechanisms, this was only done at the risk identification phase, e.g., at the outset of a project. There was mostly no documented follow-up on risk prioritization and status, assessment of effectiveness of mitigating actions, and residual risks, in either the Enhanced Results Based Management platform or in the Atlas section dedicated to recording and updating projects risks.

These findings were consistent with the issues already noted in the Operation Support Group's handover note "lessons learned on ERM implementation" from September 2011. There, it was stated that risk identification and assessment is undertaken more informally and intuitively at the project level and at the country level embedded in ongoing planning processes, project design and formulation, and on an ad-hoc basis when major risks arise. Further, the handover note mentioned that formal risk reporting through the corporate risk register (risk log) was seen to encourage discussion on risks particularly in the planning phase in Country Offices. The handover note also stated that there were little incentives for Country Offices to register their risks as the managing of risks was undertaken more intuitively.

Insufficient use of the established ERM communication mechanisms, such as risk logs and the risk tabs of the Integrated Work Plan may reduce the quality and usefulness of information gathered through the ERM process; it may thus weaken the management of risks, weaken risk-based decision-making and ultimately render the ERM mechanism less relevant, both for management and for oversight purposes.

In response to the draft audit report, management indicated that "for accountability purposes risk communication should ideally be recorded in the risk log; however, management does not agree – and it was never the intent of existing policies – to limit risk communication only to formal online channels. Speed in response to a risk escalation is essential and far outweighs any benefit of more systematic initial documentation, which might hamper the organization in managing risks effectively." Management added that there was ample evidence that risk escalation, especially in emergency situations, has been responded to effectively irrespective of the channel used to communicate. Maintaining multiple communication channels is a critical aspect of UNDP's resilience, since these redundancies ensure that risk escalation and risk response take place even when internet access is disrupted.

OAI Comment:

In view of the comments received in response to the draft report and considering the action proposed by management to implement Recommendation 2 below which would also contribute to addressing the underlying issue raised about improving communication channels, OAI is not providing a specific recommendation for this particular audit issue. However, in following up on the implementation of Recommendation 2, OAI will also assess the evidence that management mentioned in their comment above.

3. Integration of ERM processes and tools

Issue 3 Insufficient integration of ERM processes and tools

As stated in the UNDP Accountability Framework, for strengthening its accountability and transparency within the context of its decentralized structure, UNDP has established processes and tools for ERM. As further provided in the Framework, these risk management tools and processes should be integrated into one comprehensive system, enabling the organization to identify, prioritize and manage risks from all sources.

At the time of the audit, risk management tools and processes were found to be not integrated into one comprehensive system. Risk logs at different levels of UNDP were fragmented -- Integrated Work Plan risk log, Atlas risk log, corporate Excel-based risk log, and a risk log attached to the Annual Business Plan. This was also confirmed in the ERM Secretariat report to the Organizational Performance Group in September 2012 where it said: "the fact that the main risk issues arising from the Integrated Work Plan risk is already reflected in the corporate risk log raises the issue of the efficiency on having two separate systems (corporate risk log and Integrated Work Plan-based risk logs) to record risk. Therefore one of the main recommendations … is to explore the possibilities of utilizing the Integrated Work Plan as the main platform for recording and monitoring risks, including the corporate level risk, without the redundancy of a separate off-line system."

Further, OAI noted that the Annual Business Plan is derived from the Strategic Plan and operationalizes the goals as defined in the Strategic Plan. OAI reviewed the 2013 Annual Business Plan and noted that it contained a section on risks, which were identified under the lead of the Executive Office and serve as a basis for UNDP bureaux and offices when developing their Integrated Work Plans. This is in contrast to the corporate risk log, in which risks are, in principle, escalated from Country Offices to the bureaux via the Integrated Work Plan (bottom-up). OAI concluded that there was little integration between the corporate risk logs and the risk log in the Annual Business Plan.

In response to the draft report, management clarified that while they agreed on the importance of integration, they indicated that this did not necessarily imply the use of a single platform. To them, it is best practice to treat certain risks confidentially and to limit access to this information due to political and reputational sensitivities, and this is also recognized by OAI. However, management agreed that better integration needs to happen to enable learning.

The weak integration of ERM processes and tools, including risk logs, may lead to inconsistent, and/or duplicated information. In addition, risk information generated in non-integrated systems may not effectively support an aggregate, enterprise-wide view and management of risks at the appropriate levels.

Priority Medium (Important)
Recommendation 2: Harmonize and better integrate risk management processes and tools at all levels of the organization. **Responsible HQ bureau:** Bureau of Management
Management action plan: With its existing technology, UNDP is now in a position to keep data and information on the same platform with different levels of access, and consequently a new planning tool, including for the maintenance of risks, is being developed. Project risks will still be entered using Atlas, and a protocol will allow automatic data extraction from Atlas into the new planning tool. The new platform is also intended to facilitate an increased formal two-way communication. **Estimated completion date:** December 2014
OAI Response: OAI acknowledges the comments provided by management. The work with a new planning tool will be reviewed by OAI as part of its follow-up at a later stage to also assess the progress on the proposed action plan to implement the recommendation.

B. Comparison with international best ERM practices

Issue 4 Weaknesses in existing ERM policy and practices

OAI assessed UNDP's existing ERM practices, procedures and policy against internationally recognized standards of risk management, good practices of other organizations and benchmarking studies.[1] Based on this analysis and lessons learned from the implementation of ERM in UNDP since its introduction in 2007,[2] OAI identified four key principles of successful ERM implementation:

- Principle 1: Clear definition of roles, responsibilities and resources
- Principle 2: Integration of ERM with existing management and decision-making processes
- Principle 3: Usefulness and user friendliness of systems, tools and guidance
- Principle 4: Critical mass of knowledge and understanding of ERM procedures and requirements

These principles represent the key challenges in establishing ERM in UNDP as a useful and valued tool for improved decision-making, and increased operational effectiveness and enhanced risk-based internal controls. Presented below are issues identified by OAI, as they relate to the four key principles, which may guide management when revising the existing ERM policies and procedures.

Principle 1: Clear definition of roles, responsibilities and resources

The roles and responsibilities of key actors involved in the ERM process (ERM Committee and Secretariat, senior management in offices, bureaux, and other staff) are specified in the Programme and Operations Policies and Procedures and they relate, *inter alia*, to managing risks, analysing risk data and escalation of risk (cf. chapter 7.0 Roles and Responsibilities).

OAI noted that while some roles and responsibilities for risk management were defined, others were not sufficiently developed and/or implemented, leading to lack of clarity in the way ERM was integrated in the daily business functions. In particular:

(a) Country Offices and projects risk logs: While the Programme and Operations Policies and Procedures stipulate that Country Office risk management builds upon the project-level risk management process by capturing broader risks that go beyond the project level and affect the overall objectives of a Unit, they do not specify the obligations of Country Offices for monitoring project-level risks.

(b) Risk logs for global and regional projects: Global and regional projects were not sufficiently integrated into the ERM process. Out of the eight regional and global projects reviewed by OAI, only three had risks recorded in Atlas. The regional and global project managers that were interviewed confirmed that there was no official ERM monitoring mechanism with the bureaux that oversees their implementation, i.e. the Bureau for Development Policy or the Bureau for Crisis Prevention and Recovery for global projects, and the Regional Bureaux for regional projects.

[1] COSO (Committee of Sponsoring Organizations of the Treadway Commission) – Enterprise Risk Management-Integrated Framework; ISO 31000 Risk Management-Principles and guidelines; Joint Inspection Unit of the United Nations – Review of Enterprise Risk Management in the United Nations System (JIU/REP/2010/4).

[2] Cf. Elements of a Strategy for Next Generation Enterprise Risk Management (ERM) in UNDP; Lessons Learned on Enterprise Risk Management (ERM) Implementation (2008-2011); Analytical review of UNDP's risk log arising from the Integrated Work Plan 2012 exercise; Enterprise Risk Management – Briefing for the Audit Advisory Committee.

(c) Risk coordination among Headquarters bureaux: ERM roles and responsibilities between the individual bureaux were not clearly defined and ERM activities were not coordinated between them. The risks tracked by the Bureau for Development Policy and/or Bureau for Crisis Prevention and Recovery, which were of relevance to one or more Regional Bureaux, were not tracked by the latter and vice-versa.[3]

(d) Resources dedicated to ERM at the corporate level: The Programme and Operations Policies and Procedures provide that the ERM Secretariat monitors and updates the corporate risk log on an ongoing basis and ensures that risk owners report to the Organizational Performance Group on the status of risks and actions on a quarterly basis. Further, the ERM Committee ensures that the overall ERM framework is effective and relevant and being applied UNDP-wide. The ERM Committee was supported in its function by the ERM Secretariat, which was being carried out by one staff member in the Bureau of Management. At the same time, that staff member was the focal point for ERM at the corporate level, providing advice and support to bureaux and offices, updating and further developing the ERM policy, and performing quality control over all Integrated Work Plan risk logs UNDP-wide. In the role of ERM Secretariat, the incumbent was also in charge of supporting the Organizational Performance Group in ensuring that corporate risk management was conducted and that the actions to address the risks were implemented, ensuring that risks that have been escalated to the ERM Secretariat have been considered by the Organizational Performance Group, as appropriate, and responded to. In addition, the incumbent was the corporate focal point for Business Continuity Management. In OAI's view, the resources provided to ERM at the corporate level may not allow an effective discharge of the extensive tasks and responsibilities that are required to establish and maintain such critical organization-wide ERM tools and processes.

(e) Responsibility for quality of risk data: The Programme and Operations Policies and Procedures do not define responsibilities for quality control of risk data at all levels of the organization.

The ERM Secretariat prepared an analytical review of UNDP's risk log arising from the 2012 Integrated Work Plan exercise and concluded that that the current status of data indicated that the culture of risk management as well as the level of awareness across the organization was still relatively low, and recommended that there was a need to increase staff awareness and knowledge (especially for managers) on risk management.

The audit results were consistent with the assessment and conclusions in the ERM Secretariat's report. While there were attempts to improve the quality of the risk logs, OAI noted that overall, the information recorded in the Integrated Work Plan risk logs at the bureau and Country Office levels was still generally of low quality. Most risks in the risk logs did not provide essential information, such as the main causes of the risks and the potential consequences should the risks materialize. Some risks were removed from the risk logs without an indication as to the reason why (e.g. risk could be fully mitigated, objectives were changed, etc.), while other risks were re-inserted from one planning year to the next without an indication of whether planned actions were taken and without an indication of the effect expected. OAI further noted that the quality of risk logs at the project level was even of lower quality than the Integrated Work Plan risk logs reviewed (e.g. unclear risk description, lack of risk response, lack of update of risk logs, etc.). Particularly in global and regional projects, project risk logs in Atlas were oftentimes not prepared or were kept offline.

[3] As examples, the Bureau for Development Policy's Integrated Work Plan for 2013 includes strategic risks/opportunities such as "the changing aid architecture and major inter-governmental processes represents a significant opportunity to (re)position UNDP as a valued partner" and "failure to credibly capture and communicate transformational results would undermine UNDP's credibility as an up-stream partner providing high level policy advice". However, such risks are not reflected in the risk logs of any of the Regional Bureaux.

Principle 2: Integration of ERM with existing management and decision-making processes

According to a benchmarking study of the Joint Inspection Unit of the United Nations on Enterprise Risk Management in the United Nations System, the greatest benefit from applying the risk management process can be achieved by integrating it with the process of developing and approving objectives. OAI noted the following:

(a) Communication mechanisms

As described in the Programme and Operations Policies and Procedures, all planning, implementation, monitoring and evaluation, including associated decision-making, should involve a consideration of risks. Except in the context of risk escalation, the Programme and Operations Policies and Procedures do not elaborate on communication and feedback mechanisms for ERM.

Even though many of the risks recorded in the corporate risk log have an impact on operational levels, there was no systematic and regular feedback from the corporate level to the operational level (e.g. about mitigating actions taken in order to resolve risks escalated from the field to Headquarters). In several Country Offices, communication on risk management via the ERM systems was still very much a bottom-up process. The existing ERM system used for recording and escalating risks from Country Offices to bureaux (Integrated Work Plan risk logs) did not provide effective two-way communication.

The Operation Support Group's handover note also recognized this deficiency, reporting that the majority of the Country Offices contacted stressed the importance of strengthening the communication channels between Headquarters and Country Offices, particularly in terms of corporate risks.

Inadequate communication mechanisms in the ERM system may reduce the value of ERM in decision-making processes.

(b) Risk appetite

Risk appetite indicates the amount of risk that is acceptable to an organization in pursuing its objectives. It may be looked at in two different ways: when considering threats, it sets the level of exposure that is considered tolerable for an organization; when referring to opportunities, risk appetite refers to the consideration of how much an organization is prepared to actively take risk in order to achieve the potential positive outcomes. In both cases, risk appetite would give each level of the organization clear guidance on the limits of risk that they can take and thus support management in defining objectives that are in line with UNDP's mission.

The Programme and Operations Policies and Procedures include the non-prescriptive "Tips and guidelines for conducting the five steps of the Risk Management cycle" which state that to determine the appropriate actions to respond to risks, one should think about the "risk appetite/tolerance level" of the unit concerned and of UNDP. However, it does not further define and develop the concept of risk appetite/tolerance for UNDP. Nonetheless, risk appetite/tolerance of UNDP is indirectly framed through UNDP's rules and procedures.

In OAI's view, in developing the risk appetite/tolerance at the programmatic and corporate level, key actors and stakeholders of UNDP could engage in a mutual dialogue within the different programmatic environments of the organization. Potential outcomes of such consultations could be a framework on risk sharing with donors. The lack of clarity and alignment between the organization's risk appetite and its strategic and programmatic requirements may impair UNDP's ability to achieve its goals and, in the long run, render the organization significantly less effective in its development activities.

(c) ERM as a continuous process

The ERM policy stipulates that staff at all levels should be effectively managing risks on an ongoing basis with risk profiles being developed and maintained in line with UNDP's Annual Work Plans. The "Tips and Guidelines" state that it is necessary to understand that risk management is a continuous process; new risks are always emerging requiring assessment and a response. Based on the audit of selected offices and projects, as well as through the analysis of minutes of meetings of corporate groups and committees, OAI concluded that ERM was not effectively embedded as an ongoing/continuous process. The Programme and Operations Policies and Procedures do not provide guidance on how to establish ERM as a regular/continuous process. In OAI's view, this could be done by, for example, by requesting that risk logs be updated on a quarterly basis, by including risk management on the agenda of regular meetings at different levels of the organization, and by providing regular reporting.

Principle 3: Usefulness and user-friendliness of systems, tools and guidance

OAI noted the following issues related to the ERM policy, guidance and tools:

(a) The ERM policy was issued on 23 February 2007, and was last reviewed on 10 February 2011. It was intended to be reviewed on 30 July 2012, but this did not occur.

The supplementary guidance 'Tips and Guidelines" on conducting the five steps of the risk management cycle state that for determining the appropriate actions to take to respond to risks, one potential option is to stop the risk from occurring or preventing it from having an impact (prevention). The guidance does not further explain the possible risk prevention measures that could be taken (e.g. changing objectives when the risks cannot be mitigated and are above the risk tolerance of the organization). In practice, this could mean adjusting project/programme/unit objectives as a result of the risk management information.

(b) Some of the guidance and requirements in the Programme and Operations Policies and Procedures and the supporting "Tips and Guidance" were vague, incomplete and contradictory in some cases. In particular:

- The Programme and Operations Policies and Procedures state that an offline Microsoft Word risk log may be created on a Country Office level for documenting sensitive risks. It states that in this case, a process for ensuring adequate response to the risk should be established. No further guidance is provided, e.g. on how to escalate such risks as they are not recorded in the Integrated Work Plan and are not managed through the system embedded escalation mechanism.

- The Programme and Operations Policies and Procedures do not define or distinguish between inherent and residual risk. Inherent risk is the risk faced by an entity in the absence of any actions taken by management and informs the organization on its risk exposure in case controls should fail. Residual risk is the risk that remains after management's response to the risk and enables the organization to assess whether there are sufficient or too many controls in place and if there is a need to re-allocate resources based on its risk appetite. If no distinction is made between inherent and residual risks, their aggregation may not serve as a reliable basis for assessing the existing status of risks that the organization faces and deciding on further responses that may be needed.

(c) The risks contained in the Integrated Work Plan are mostly risks that were relevant to operations. Risks corresponding to the programmatic objectives of UNDP were mentioned only in few cases. This also applied to the risk log prepared for the Annual Business Plan.

With regard to risk logs, OAI noted missing elements and inadequacies within and across the different risk logs used at different levels of the organization:

- *Integrated Work Plan risk log:*
    - The formulation of risks was not standardized and often insufficient (it often lacked sufficient information regarding the risk/event, the cause and the consequence). The consequences may be reported in the "potential impact" field; however, OAI noted that this was not consistently done. The template and the instructions did not provide sufficient guidance on the formulation of risks.
    - There was no field to indicate the risk typology, such as strategic, financial, operational, etc. In OAI's view, this information is important for aggregating and analysing risks. There was no dedicated field to report on existing status of risks, where it could be described what effect mitigating actions have been taken so far, and what more may need to be done.
    - A field for timelines/deadlines for implementing risk responses was missing.
    - There was no field to mark potential cross-cutting/horizontal risks.
    - The risk owner must be identified by name in the risk log, however, in OAI's view, the risk owner should be specified by function in order to ensure continuity in case of staff changes.
    - There was no reference to inherent and residual risks.
    - The difference between the status fields 'continue monitoring' and 'requires action' was unclear. In many cases sampled, the status 'continue monitoring' was ticked even when the response field specified mitigating actions.

- *Project risk log (Atlas):*
    - The online version and the offline project risk log had different structures and elements.
    - The guidance on the use of the critical flag field, which should be ticked if the impact and probability of risks are high, was not sufficiently clear. OAI noted that it was very rarely used and did not trigger any automatic notifications or actions at any level (compared to the escalation mechanism established in the Integrated Work Plan risk log).

- *Corporate risk log:*
    - Elements not included in the corporate risk log were: impact/likelihood, inherent/residual risks, deadlines/milestones for mitigating actions, and risk response type (avoid/transfer/reduce/accept), which are fundamental to specifying risks.
    - The origin of the risk (top-down vs. bottom-up reporting) was not stated. This information would support effective communication at later stages of managing and mitigating risks.

Particularly with regard to the Atlas project risk logs, OAI also noted complaints regarding the usability and intuitiveness of the tool. The lack of sufficient, clear, concise and up-to-date ERM policy, guidance and tools may lead to ineffective risk management in different levels of the organization.

Principle 4: Critical mass of knowledge and understanding of ERM procedures and requirements

UNDP provides online training on ERM. This training is not mandatory for staff/management. OAI noted that its content is a basic introduction to risk management, and may not sufficiently meet expectations of staff in the field. From its audit sample, OAI noted that some specific needs expressed by the offices and projects were not sufficiently covered in the available training on ERM (e.g., potential legal risks and project related risk management). Further, it was stated by the offices and project representatives interviewed that the training was very theoretical and did not provide practical guidance for understanding and applying UNDP's ERM approach.

OAI also analysed the completion rate of ERM training over the last several years and noted a significant decrease in participants: 2008 (473 individuals), 2009 (221), 2010 (159), 2011 (62), 2012 (48), and 2013 (17).

Project related risk management has been part of PRINCE 2 training. According to the Bureau of Management, UNDP adopted PRINCE 2 principles and thus, also adopted risk management for projects. OAI noted that, similar to the completion rates for the specific ERM training, the number of staff that had completed training in PRINCE 2 for project management had significantly decreased over the last years (i.e., 1,940 participants in 2006 and 220 in 2012).

The significant decrease in training in ERM and in PRINCE 2 would have been understandable had ERM reached a good level of maturity in UNDP and had been effectively mainstreamed in the organization.

OAI noted in the Operation Support Group's handover note a recommendation to establish a network (teamwork space) where staff can exchange good practices and experiences, and establish links to training materials on risk management. However, at the time this report was being drafted, this suggestion had not yet been implemented. In OAI's view, a moderated community of practice could support a better and wider understanding and sharing of risk management practices in the decentralized structure of UNDP.

In response to the draft report, management expressed its appreciation of the suggested future improvements to UNDP's policy, tools and practices on ERM and its understanding that these future improvements go beyond the scope of UNDP's existing procedures and systems as assessed by OAI. Management added that the existing ERM system introduced in 2007, together with preceding and other concurrent formal and informal risk management processes, has served the organization to effectively manage risks.

In conclusion, through the comparison of UNDP's existing ERM practices, procedures and policy with international standards on ERM, best practices and the lessons learned over the past six years, the audit revealed the need to fundamentally revisit the policy and practices of ERM in UNDP and to address the issues mentioned. This review should also take into account the changing business model of UNDP, the new Strategic Plan and the variety of technological tools available to management and staff.

Priority High (Critical)

Recommendation 3:

Building on lessons learned from the Enterprise Risk Management implementation since 2007, best practices and standards, as well as the changing business model of UNDP, new Strategic Plan and availability of various technological tools, UNDP should redesign the related policy, tools and practices, as appropriate, and identify the level of resources that would be necessary for a successful organization-wide update and maintenance.

Responsible HQ bureau: Bureau of Management

Management action plan:

Management will conduct a thorough review of the existing ERM system and compare it against a recognized international standard. Recommendations from such a review, together with this audit report, will be the basis for revising the existing system.

Estimated completion date: December 2014

ANNEX 1: Definitions of audit terms - ratings and priorities

A. AUDIT RATINGS

- **Satisfactory** Internal controls, governance and risk management processes were adequately established and functioning well. No issues were identified that would significantly affect the achievement of the objectives of the audited entity.

- **Partially Satisfactory** Internal controls, governance and risk management processes were generally established and functioning, but needed improvement. One or several issues were identified that may negatively affect the achievement of the objectives of the audited entity.

- **Unsatisfactory** Internal controls, governance and risk management processes were either not established or not functioning well. The issues were such that the achievement of the overall objectives of the audited entity could be seriously compromised.

B. PRIORITIES OF AUDIT RECOMMENDATIONS

- **High (Critical)** Prompt action is required to ensure that UNDP is not exposed to high risks. Failure to take action could result in major negative consequences for UNDP.

- **Medium (Important)** Action is required to ensure that UNDP is not exposed to risks that are considered moderate. Failure to take action could contribute to negative consequences for UNDP.

- **Low** Action is desirable and should result in enhanced control or better value for money. Low priority recommendations, if any, are dealt with by the audit team directly with the Office management, either during the exit meeting or through a separate memo subsequent to the fieldwork. Therefore, low priority recommendations are not included in this report.