United Nations
Educational, Scientific and
Cultural Organization

Organisation
des Nations Unies
pour l'éducation,
la science et la culture

Organización
de las Naciones Unidas
para la Educación,
la Ciencia y la Cultura

Организация
Объединенных Наций по
вопросам образования,
науки и культуры

منظمة الأمم المتحدة
للتربية والعلم والثقافة

联合国教育、
科学及文化组织

Internal Oversight Service
Audit Section

IOS/AUD/2016/05
Original: English

Advisory on UNESCO's Enterprise Risk Management

July 2016

Auditors:
Sameer Pise
Dawn Clemitson
Christian Muco

EXECUTIVE SUMMARY

Key results

In an advisory capacity, the Internal Oversight Service assessed the design and functioning of UNESCO's Enterprise Risk Management (ERM).

UNESCO applies a number of good risk management practices, including: (i) programme managers assessing delivery risks as part of planning and budgeting, (ii) managers across the organization assessing and attesting annually to the effectiveness of internal controls under their responsibility and (iii) several management committees identifying and addressing a range of risks against predefined risk tolerances. In addition, UNESCO has established a Risk Management Committee, disseminated a Risk Management Training Handbook, conducted a training session for Heads of Field Offices, and identified and discussed key corporate risks at a recent Senior Management Team retreat.

However, progress has been sporadic and, when benchmarked against standardized maturity models, UNESCO's ERM practices are at a relatively low level (i) with basic ERM practices in place and (ii) currently transitioning to a more formalized and systematic approach. As part of this engagement, IOS identified a number of near-term actions to strengthen ERM. Specifically, the Risk Management Committee should:

- Convene regularly and perform its coordination role
- Finalize a Risk Management Policy for adoption by the Organization
- Re-examine current corporate risks and, in consultation with senior management, update the risk register accordingly
- Articulate UNESCO's risk appetite' in consultation with senior management, for presentation to the Executive Board
- Revise and clarify the Committee's terms of reference to support its effective functioning
- Determine and request the resources needed to advance UNESCO's ERM
- Engage the Organization's existing risk management architecture to support a better flow of risk information
- Introduce periodic risk reporting to the senior management and Executive Board

Once in place, a robust ERM will help UNESCO better understand and more effectively respond to risks and opportunities facing the Organization in achieving its objectives.

Background

1. Enterprise Risk Management (ERM) is a structured, consistent and continuous process across an Organization for identifying, assessing, communicating and responding appropriately to opportunities and threats that affect achievement of the Organization's objectives.

2. ERM at UNESCO originated in November 2008 when the College of ADGs endorsed the establishment of a Risk Management Committee. Under the leadership and support of the Bureau of Strategic Planning (BSP), this committee was mandated to consolidate risk information from ongoing assessments and to transform risk management into a continuous process in UNESCO.

3. The Risk Management Committee identified and discussed UNESCO's top risks and also requested Headquarters and Field Offices to develop and maintain risk registers. BSP also introduced risk management training and published a risk management handbook. The Committee was active until the end of 2013.

4. UNESCO's Oversight Advisory Committee, in June 2015, while recognizing initial progress, recommended that ERM be further strengthened and revitalized. Subsequently, the Director-General established a new risk committee in July 2015 with a mandate to (i) strengthen

UNESCO's ability to deliver agreed results, (ii) embed a culture of risk-informed decision-making and (iii) mainstream risk management as part of work-planning, results monitoring and reporting. The Director of BSP is the responsible officer for ERM and chair of the new Risk Management Committee. A part-time secretariat in BSP supports the Risk Management Committee.

5. UNESCO's Executive Board is following risk management in the wider context of the ongoing governance reform. At its 199th session, the Board requested the Director-General to report at its next session on progress made towards establishing a global risk register. Further, the Oversight Advisory Committee presented information to Member States on the functions of audit and risk committees in public sector organizations at a meeting in June 2016.

Scope, Objective and Methodology

6. This IOS advisory engagement assessed the design and functioning of UNESCO's ERM processes with the objective of determining its current maturity level and identifying opportunities for improvement. The engagement scope focused on processes of risk identification, assessment, response and communication.

7. The engagement was performed in accordance with the *International Standards for the Professional Practice of Internal Auditing* and applied selected criteria set forth in COSO's[1] *Enterprise Risk Management – Integrated Framework* and ISO 31000:2009[2] *Risk management – Principles and guidelines*.

8. As part of the engagement methodology, IOS:

- Assessed UNESCO's risk management practices using standardized maturity models of the Institute of Internal Auditors (IIA) and of the professional body for Chartered Global Management Accountants (CGMA);
- Benchmarked UNESCO's risk management policy, resource allocation and terms of reference of the Risk Management Committee to those of other UN organizations and suggested amendments and inclusions;
- Interviewed managers at Headquarters, Field Offices and Category I Institutes;
- Reviewed minutes of the Risk Management Committee, the risk management handbook and risk identification mechanisms;
- Took stock of UNESCO's risk architecture including UNESCO's management committees and their potential ERM contribution;
- Proposed an escalation process for consolidating UNESCO's risk information;
- Identified the elements for determining and articulating UNESCO's risk appetite.

9. IOS consulted with the Chair and Secretariat of the Risk Management Committee while developing the engagement deliverables that are attached as appendices to this report.

Achievements

10. UNESCO applies a number of good risk management practices. These include:

At programme planning and implementation level:

- Programme Sectors, Corporate Services and Field Offices assess programme delivery risks when preparing the Programme and Budget (C/5);
- Responsible Officers periodically report implementation challenges and remedial actions in the Programme Implementation Report;
- Project Officers are to factor risks when planning extrabudgetary projects;
- An initiative is underway to more systematically assess high-risk projects prior to their approval.

[1] Committee of Sponsoring Organizations (COSO) of the Treadway Commission broadened its earlier guidance on internal control frameworks to a more holistic enterprise risk management framework.
[2] ISO 31000:2009, promulgated by the International Organization for Standardization, sets forth principles, framework and process for managing risk applicable to both private and public organizations.

At entity level (i.e., Sectors, Services, Field Offices and Category 1 Institutes):

- ADGs, Directors and Heads of Office annually self-assess internal controls under their responsibility. This exercise helps identify control gaps and areas where risks are not effectively mitigated;
- As an emerging practice, some UNESCO Directors/Heads of Office compile risk registers specifying risks and mitigation plans relevant to their operations;
- For Directors/Heads of Field Offices, management responsibilities specifically include risk management.

At organization level:

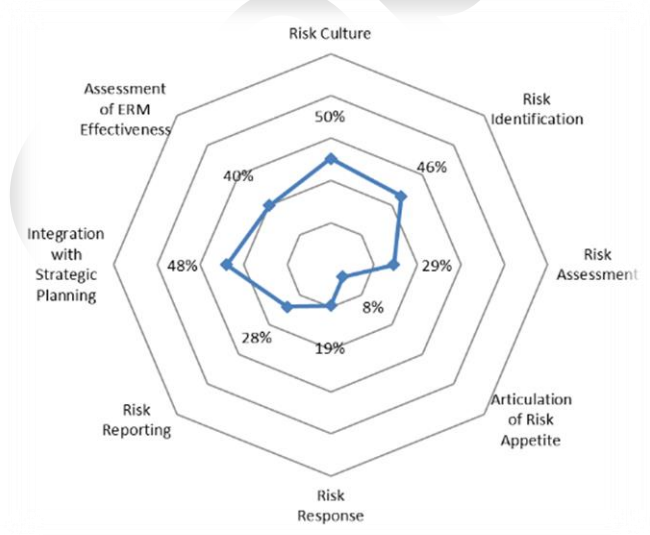
- The Risk Management Committee and Senior Management Team have undertaken exercises to identify and address top corporate risks, exercises which now need to be better institutionalized in the risk management framework;
- The Risk Management Committee Secretariat developed a risk management handbook as an Organization-wide reference and for training purposes and conducted a training session of Heads of Field Offices;
- Risk awareness is increasingly reflected in corporate policies and risks are often identified, assessed and communicated when planning change initiatives;
- Measures are being introduced to strengthen the senior-level coordination and management action on all oversight recommendations;
- The Oversight Advisory Committee, per its terms of reference, periodically reviews and advises on the Organization's risk management practices.

Challenges

11. Notwithstanding the above progress, UNESCO's ERM practices need to advance considerably in order to embed a robust and relevant risk management framework. Assessment through two common maturity models (IIA and CGMA) illustrates current status (see Figure 1).

Figure 1 – Assessment of UNESCO's ERM Processes

CGMA maturity model assessment



Description of Current State of ERM	Range of Total Score
Just Getting Started	From 1 to 25
Basic ERM Practices in Place	From 26 to 45 ← UNESCO
Basic as well as some more sophisticated ERM Practices in Place	From 46 to 65
Robust ERM in Place	From 66 to 75

IIA maturity model assessment

12. Based on our assessment, the following nine short-term actions will substantially advance risk management in UNESCO.

Action 1: The Risk Management Committee to regularly convene and perform its coordination role

13. The Terms of Reference of UNESCO's Risk Management Committee (DG Note14/15 of June 2015) state that the Committee is to meet as required to fulfil its remit, but no less than once every two months, and submit periodic reporting to the Senior Management Team.

14. Since its re-establishment in July 2015, the Committee has met twice, in January and July 2016. The Committee is yet to establish its authority and exercise the foreseen coordination role in advancing risk management. Further, risk information has largely remained static with the Committee relying on a corporate risk register that has not substantively evolved since 2012.

15. Regular meetings based on a clear timetable or calendar of work are needed for the Committee to take proactive steps in fulfilling its mandate.

Action 2: The Risk Management Committee to finalize the draft Risk Management Policy and present it to the Director-General for approval

16. To ensure consistent understanding and application, Organizations seeking to set up coordinated activities to manage risks should establish a Risk Management Policy.

17. UNESCO's Risk Management Policy is in draft form and is not yet endorsed by the Risk Management Committee. As part of this advisory engagement, IOS compared an initial draft policy prepared for the Risk Management Committee to the relevant policies of several other organizations[3] and considered industry standards.[4] This content analysis led to a number of suggestions for improving the initial draft policy:

- Introduction: Reflect UNESCO's current context in the risk policy by linking organizational objectives and risk management.
- Risk Appetite: Articulate in the policy or provide reference to UNESCO's risk appetite statement.
- Definitions: Include in the policy definitions of commonly used risk terms to promote consistent understanding.

[3] UNICEF, WFP and UNDP
[4] ISO 31000:2009, *Risk Management – Principles and guidelines* and COSO guidance

- Principles: Make specific reference in the policy to (i) senior management's commitment to make necessary resources available for ERM, (ii) consolidation and escalation of risk information from various sources and (iii) the Risk Management Committee's responsibility to periodically review and improve the risk policy and framework.
- Risk Categorization: An Organization-wide risk management framework requires common understanding of risk categories. For reference, IOS has compiled a table of risk categories (Appendix 1) that can be considered by the Risk Management Committee when defining UNESCO's risk categories for inclusion in the policy.

18. Appendix 2 presents a revised draft Risk Management Policy reflecting IOS' proposals for consideration and, if desired, further refinement by the Committee.

Action 3: The Risk Management Committee to re-examine and update the current corporate Risk Register to reflect potential future events

19. The ISO standards define risk as the effect of uncertainty on objectives, which is often characterized by reference to potential future events and their consequences. Risks should be identified as events that are yet to occur and may impact achievement of the Organization's objectives. Further, risk management should be dynamic, iterative and responsive to change. As external and internal events occur, new risks emerge, some change and others disappear.

20. The most recent corporate Risk Register (February 2015) often lists past events or current conditions as risks. For example:

- The breadth of UNESCO's mandate poses special challenges, complicated by an inability to articulate well and focus on priorities.
- Difficulty to implement projects and demonstrate quality results and impact, especially at country level.
- Non-payment of the US contribution, uncertainty to ensure a sustainable level of extrabudgetary funding (including Emergency Fund)

21. IOS also notes that risk identification has largely been stagnant, with little evolution of the top risks since 2008 (see Table 1 below).

Table 1 – Comparison of UNESCO's corporate Risk Registers for 2008, 2012 and 2015

2008	2012	2015
Resourcing of UNESCO's programmes: Uncertainty about future levels of regular budget funding, coupled with a broadening range of responsibilities.	Non-payment of the US contribution, uncertainty to ensure a sustainable level of extrabudgetary funding (including Emergency Fund)	Non-payment of the US contribution, uncertainty to ensure a sustainable level of extrabudgetary funding (including Emergency Fund)
Governance: A tendency on the part of the Secretariat to present issues in a positive light and to make overly-optimistic commitments. Lack of confidence in the Secretariat by the Member States may lead to overly intrusive governance processes and micro-management		
Staffing: Lack of definition of our requirements in terms of staff profile and competencies may inhibit our ability to attract/deploy/support staff appropriately	Ineffective management of occupied and vacant posts in correlation with priorities, taking into account financial constraints	Ineffective management of human resources, including ad-hoc management of vacant posts (instead of strategic), leading to a mismatch between staff profiles and the strategic and programmatic priorities of the Organization
Organizational design and accountability: The current architecture, mechanisms and support structures governing decentralization may impact on our ability to deliver effectively at the country level and be an active participant in UNCTs.	Difficulty to implement projects and demonstrate quality results and impact, especially at country level	Difficulty to implement projects and demonstrate quality results and impact, especially at country level
Corporate systems: Corporate information systems and network applications that are not fit for purpose		

Financial Management: An inability to identify all relevant cost components and to track funding appropriately. Lapses in procurement procedures may result in negative publicity and loss of organizational credibility. Qualified accounts by the external auditor may result in lack of confidence by the Member States		
RBM Quality or programme delivery and visibility: The breadth of UNESCO's mandate poses special challenges, complicated by an inability to articulate well and focus on priorities	The breadth of UNESCO's mandate poses special challenges, complicated by an inability to articulate well and focus on priorities	The breadth of UNESCO's mandate poses special challenges, complicated by an inability to articulate well and focus on priorities
Delivering within the UN System: Inability to fulfil commitments and effectively participate in UN reform processes	Losing the opportunity to reform the organizational design towards challenges, a fortiori at the Field level	Losing the opportunity to reform the organizational design towards challenges, a fortiori at the Field level

22. Effective risk identification and articulation, including emerging risks, facilitates the effective avoidance of or response to those future events should they occur.

Action 4: The Risk Management Committee, in consultation with the Senior Management Team, to articulate UNESCO's risk appetite and communicate it to the Executive Board

23. UNESCO's Risk Management Training Handbook defines risk appetite as the amount of risk that is judged to be tolerable and justifiable by senior management. Risk appetite is not constant and is informed by changing variables. A risk appetite statement clarifies the permissible levels of enterprise risks, which include:

- risks that can be taken because they are sufficiently mitigated;
- undesirable risks that should be avoided and for which zero or very low tolerances should be set;
- strategic, financial and operational thresholds providing a framework within which the Organization can take risks.

24. At the operational level, risk appetite dictates operational constraints for routine activities. At the senior management level, risk appetite translates into a set of procedures to ensure that risks receive adequate attention when making tactical decisions. Once established and endorsed at the governance level, risk appetite can be an effective driver of strategic risk decisions.

25. While UNESCO is yet to formally articulate its risk appetite, some elements of risk tolerance are present in administrative guidance (e.g., UNESCO's Investment Policy specifies permissible investment parameters, and monetary thresholds are established guiding the level of risk taking associated with contracting). Appendix 3 provides further elaboration of instances where UNESCO as articulated elements of risk tolerance levels. It is worth noting that articulation of risk appetite is an emerging practice within the UN system organizations, and examples from other organizations (e.g., WFP and WIPO) are available on public internet for consideration by the Risk Management Committee.

26. It is particularly important to remain focused on engaging with the governing bodies in establishing risk appetite at the strategic level and ensuring that working methods include assessing risks as an integral part of strategic decision-making of the governing bodies. Recognizing the responsibilities of the governing bodies in this regard, the Oversight Advisory Committee briefed Member States in June 2016 on the scope and purpose of Audit and Risk Committees, providing background information on assurance and risk management mechanisms and explaining the functions of Audit and Risk Committees at the governance level. Following up on this, the Risk Management Committee should ensure that its work in articulating risk appetite takes account of the strategic responsibilities and needs of the governing bodies in order to foster a more holistic approach to risk management in UNESCO.

Action 5: The Risk Management Committee to revise its Terms of Reference to clarify its mandate and submit for approval of the Director-General

27. The Terms of Reference for Risk Management Committees should sufficiently describe the Committee's purpose and structure to support efficient and effective ERM processes.

28. As part of this advisory engagement, IOS assessed the current Terms of Reference of the Committee as established in June 2015 and compared the content to other relevant models (e.g., UNDP and the model of the Institute of Chartered Secretaries and Administrators). This content analysis led to a number of suggested revisions to the current Terms of Reference:

- Purpose and scope: Include in the Committee's purpose the: (i) implementation and monitoring of risk management, (ii) risk management awareness and (iii) maintaining the Organization's risk profile;
- Composition and structure: (i) Add the Legal Advisor and ODG/FSC as members of the Committee, and ensure Headquarters and Field Security are duly represented by ERI; (ii) Clarify role and participation of Sectors, Services and Field Offices (i.e., senior-level risk focal points); and (iii) define a risk escalation process;
- Frequency and agenda of meetings: Add a provision on quorum and standing agenda items for the Committee meetings;
- Functioning / responsibilities: Clarify the Committee's advisory, monitoring and coordinating responsibilities;
- Authority: Add a provision on the Committee's authority to seek information, advice and attendance of staff as and when required;
- Reporting responsibilities: Add provision on periodically reporting key corporate risks to the Executive Board.

29. Proposed or illustrative revisions to the current draft Terms of Reference are annexed to the Risk Management Policy in Appendix 2 of this report.

Action 6: The Risk Management Committee to determine the appropriate level of investment and present a proposal to the Director-General

30. The ISO risk management standards state that effective risk management requires adequate resources to support the following necessary elements:

- people, skills, experience and competence
- processes, procedures and tools
- information and knowledge management systems and
- training programmes.

31. UNESCO's startup investment for ERM has been very low when compared to other organizations. The JIU review of ERM in the United Nations (JIU/REP/2010/4) assessed the cost of ERM implementation across the participating organizations, for example, and noted that UNESCO relied on existing staff structures while most other organizations reported specific resource allocation (ranging up to US $3.1 million) for ERM implementation.

32. UNESCO's current staff-time allocation to ERM continues to be too low. The DIR/BSP chairs the Risk Management Committee in addition to undertaking other important roles. Two staff in BSP's Section for Budget and Risk Management reportedly dedicate approximately five percent of their time as the Committee's Secretariat, which is not sufficient to substantively progress with ERM. While there is complementarity between strategic planning and risk management, IOS believes that the current placement of the Committee's Secretariat in a small team comprised of budget officers creates a perception that the focus of risk management is on budgetary and financial risks rather than on enterprise-wide risks.

33. This limited resource allocation in light of many competing priorities has had consequences. The Risk Management Committee rarely convenes, the corporate Risk Register is not updated and only eight Field Offices have compiled risk registers.

34. The Oversight Advisory Committee recommended[5] in June 2015 that the Director-General consider appointing a Senior Risk Officer, at a sufficiently high level (such as direct reporting to the Director-General) who is well qualified in risk management policy and process and that this person also be charged with the Secretariat function for the Risk Management Committee.

35. IOS estimates that the Secretariat will require, at a minimum, a dedicated professional staff with proven risk management competencies to support the coordination of risk information, train staff, maintain risk management tools and otherwise support the functioning of the Risk Management Committee. Together with the establishment of adequate in-house capacity, IOS advises in line with the recommendation of the Oversight Advisory Committee that the Risk Management Committee also seek resources for temporarily engaging a qualified risk management consultant to accelerate this current phase of advancement. Such expertise in the short-term can guide the Committee by further elaborating and introducing a systematic approach to identify, assess, manage and communicate corporate risks.

Action 7: The Risk Management Committee to better engage UNESCO's existing risk management architecture

36. The ISO risk management standards state that an organization should establish internal communication and reporting mechanisms to escalate and consolidate risk information from across the organization. Risk identification is impaired when information from various sources is not consolidated.

37. Management Committees: UNESCO has a number of silo-based, though often robust, risk management mechanisms in place. Most notably, management committees play important roles in monitoring and mitigating risks. These include the following:

- Programme Management Committee
- Contracts Committee
- Investment Committee
- Knowledge and Information Technology Advisory Board
- UNESCO Publication Board
- Advisory for Works of Art
- Consultative Committee on Health, Safety and Ergonomics.

38. However, there are no established channels for the committees to communicate relevant risk information to the Risk Management Committee. Such communication should include escalation of significant unmitigated risks and a periodic statement of the management committees that risks under their respective purview are appropriately identified, assessed and managed within the prescribed tolerance levels.

39. To facilitate the above communications, draft text is outlined in Appendix 4 for inclusion in the Terms of Reference of the relevant management committees.

40. Risk Information Flow: IOS also mapped existing risk information sources and illustrated a proposed information flow (see Appendix 5). The critical elements are that:

- Headquarters Sectors and Services reliably and timely communicate significant unmitigated risks associated with their respective mandate to the Risk Management Committee and
- Field Offices communicate their significant unmitigated risks through a central point, such as ODG/FSC, where the risks can be considered and consolidated as appropriate for transmission to the Risk Management Committee.

41. IOS proposes that responsibilities for identifying and communicating significant unmitigated risks be formally established as follows:

[5] Recommendation No. 9 of the OAC's June 2015 Report

- For Headquarters Sectors and Services: Either the principal officer (ADG / Director) or a designated senior-level focal point;
- For Field Offices and Category 1 Institutes: The principal officer (Director / Head of Office).

Action 8: The Risk Management Committee to introduce systematic reporting of corporate risks to the Senior Management Team, Director-General and Executive Board

42. The current Terms of Reference of the Risk Management Committee require that the Committee (i) regularly report to SMT on critical risks, (ii) report on its performance and effectiveness and (iii) provide a statement on the adequacy of the Organization's management of risk. These are relevant and appropriate measures, though are yet to be implemented.

43. In addition to the above, the guidance promulgated by ISO and by COSO highlight the role of the governing body in effective risk management at the strategic level by citing, among other things, the need of the governing body to understand the most significant risks faced by the organization.

44. The Executive Board has expressed increasing interest in risk management and, most recently, has requested that the Secretariat report in October 2016 on the progress achieved in establishing a global risk register. Member States also requested a briefing by the Oversight Advisory Committee in June 2016 on the scope and purpose of Audit and Risk Committees at the governance level.

45. Based on the above, the Risk Management Committee should anticipate the periodic presentation of key corporate risks to the Executive Board and institutionalize such reporting, through the Director-General, as part of its Terms of Reference

Action 9: Other opportunities for improvement

Updating and disseminating the Risk Management Training Handbook

46. In 2010, BSP published and disseminated in printed copy as well as digitally a Risk Management Training Handbook. This was an important step in advancing risk management practices in UNESCO. More can be done to make this document a consistent reference, such as incorporating it by reference as a part of UNESCO's Administrative Manual. Directors and Heads of Field Offices informed IOS that the handbook is Headquarter-centric and needs to be updated for better risk management guidance to cope with operational challenges in the field. In absence of such guidance on managed risk-taking, staff can be risk averse and their responses to risks can be ad hoc and reactive.

47. Accordingly, the Secretariat of the Risk Management Committee should update the Handbook based on insights gained during the past five years and disseminate it widely as part of UNESCO's formal procedures and guidance as consolidated in the Administrative Manual.

Aligning current initiatives

48. Since 2011, UNESCO has embedded the good practice of annual Control Self-Assessments whereby all Sectors, Services, Field Offices and Category 1 Institutes self-assess their respective control processes using a standardized tool and assessment scale. BFM coordinates this annual exercise, achieving a high participation rate and increasingly reliable and relevant assessment results. It should be noted that IOS developed the initial assessment tool based on UNESCO's internal control framework, and both IOS and the External Auditor examine the reliability of these self-assessments where relevant in undertaking audits.

49. In 2013 and 2014, BSP encouraged Field Offices to undertake risk identification and assessment exercises and to develop risk registers for each Office. This initiative has progressed slowly, with only eight Field Offices developing risk registers. (As a separate exercise, in 2015 twelve Field Offices and seven Headquarters Sectors and Services identified and assessed risks specifically related to budget scenarios for the 38 C/5.)

50. IOS notes substantial potential synergy between the annual Control Self-Assessment exercise, which is well advanced, and the development of risk registers at the level of the various operating units, which is lagging. Both of these exercises identify risk and control information through separate efforts. Evolving the current control assessment into a risk and control assessment, leading to the formulation of risk registers, presents a good opportunity to advance ERM practices in UNESCO. Accordingly, IOS reiterates its earlier advice that these exercises be consolidated.

Supporting effective change management practices

51. Risks identified at the organizational level are often addressed by launching corporate change initiatives. Where such initiatives are planned and undertaken to mitigate corporate risks identified and monitored by the Risk Management Committee, the Committee should ensure sound change management practices are followed including establishment of clear roles, accountabilities, timeframes and budgets to achieve the intended deliverables or results. By promoting these practices, the Committee can contribute to a culture of effective change management in UNESCO.