UNITED NATIONS SYSTEM CEB

Chief Executives Board for Coordination

CEB/2020/HLCM/4
24 April 2020

HIGH-LEVEL COMMITTEE ON MANAGEMENT (HLCM)
Thirty-Ninth Session

Guidance Note - Embedding Risk Management

Background

1. At its 35th session in April 2018, HLCM examined how United Nations system organisations have been developing and putting in place risk management tools and frameworks to reform management processes, improve efficiency and bring greater value in support of the 2030 Agenda for Sustainable Development. The Committee agreed on the need for joint, cross-functional engagement towards the system-wide harmonisation of risk management practices and endorsed the attached Terms of Reference (TOR) for a Task Force (TF), to be co-chaired by WIPO and WFP.

2. The TF included those organisations who responded to a call for nominations or requested to join, and by December 2019 included FAO, IAEA, ICAO, IMF, IFAD, ILO, IOM, OCHA, OECD, UN Secretariat, UN DSS, UNAIDS, UNDP, UNEP, UNFPA, UNHCR, UNICEF, UNIDO, UNOPS, UNRWA, UN WOMEN, WFP, WHO and WIPO. The TF is also committed to interact and consult with UN Representatives of Internal Audit Services (UN-RIAS) to ensure benefit would be derived from their input and contributions.

3. The TOR called for '*Develop guidance on how a UN system organization may approach the establishment of key organizational risk management approaches, to include... embedding risk management into performance/planning processes.'*

Working Modalities

4. For practical purposes, members of the TF self-selected area(s) of prioritised interest, which created the sub-groups, each supported by a facilitating organisation. Plenary meetings of the full TF were held monthly, to ensure broad engagement in discussions on various aspects of the guidelines and information sharing. UN RIAS was also represented at TF meetings and provided valuable input on specific matters, which were taken duly into account in finalising the guidelines.

5. The globally located TF operated without any formally allocated budget, and as such worked almost exclusively via remote working approaches (videoconference, email, etc.). While this was a cost effective solution for rapid and results-oriented delivery, it presented certain logistical and practical challenges. However, the active engagement and collaboration of members ensured that the TF arrived at an agreed guidance document.

6. The 'Embedding Risk' sub-group, initially met virtually in addition to the plenary sessions, taking a collaborative approach. In order to achieve as wide a representation as possible, the paper was then drawn into the plenary, where all TF organisations' perspectives, case studies and comments were discussed and incorporated.

7. **Once in a state of final draft, the paper was sent to the informal UN Strategic Planning Network at their meeting in December 2019. Comments that resulted from the discussion and review were incorporated as possible and feedback provided on all comments from all organizations.**

Embedding Risk Management Guidance Note

8. HLCM members have emphasised the need to ensure that risk management takes root in their respective organisations (Section 1). The challenges organisations face in accomplishing this are those of cultural change and making risk management a reflex as opposed to 'ticking the box' and focusing excessively on process.

9. The present responds to the HLCM's request and sets out to accomplish two goals: Firstly, to establish the importance of integrating risk management with performance management processes (Section 2) and in doing so provides an overview and case studies of how organisations have achieved success in this area.

10. Secondly, the paper collates nine enablers (Section 3), developed collaboratively by different organizations and often using case studies to demonstrate the value. These enablers are a menu of ways that risk management can become truly embedded in an organization. It is not to say that every organization should implement all of the following nine approaches, however, they may be worth considering:

    (i) Combine formal and informal mechanisms
    (ii) Strengthen risk capabilities
    (iii) Build a network of risk ambassadors
    (iv) Focus on user experience and value add
    (v) Reinforce the link between internal controls and risks
    (vi) Consider risks as potential opportunities
    (vii) Focus on new and emerging risks
    (viii) Apply risk data to support change initiatives
    (ix) Strengthen risk culture

11. **It should be emphasised that while this present document provides key approaches to embed risk management in the programme management cycle, and offers a series of enablers to effectively embed risk management in the organization's culture, it is intended to be guiding rather than prescriptive in nature.**

Proposed Decision

12. The HLCM is invited to consider and endorse the Embedding Risk Management Guidance, to be used as a practical guide to help organisations ensure that risk management becomes an organizational reflex.

HLCM Cross-Functional Task Force on Risk Management

Guidance Note – Embedding Risk Management

Benefits and practicalities of integrating ERM with the Enterprise Performance Management process

April 2020

UNITED NATIONS SYSTEM

1 Table of Contents

1. Introduction

1.1 Background and purpose of this paper

At its 37th session in April 2019, the High-Level Committee on Management (HLCM) mandated the Cross-Functional Task Force on Risk Management (hereafter 'the Task Force') to develop guidance for UN organisations to truly embed risk management into their respective organisation, including the benefits and practicalities of integrating with the programme management cycle. This document is intended to help highlight actions and areas (based on lessons learned, and practical experiences of various organisations across the UN system) which can help to make risk management an integral part of decision-making and performance management.

A survey sent in December 2018 to UN agencies participating in the Task Force found that whilst over 80 per cent of respondents identified a relationship between the risk process and the strategic planning process, less than half reported an effective association with performance monitoring/evaluation and budgetary planning. Furthermore, and despite recognition of the importance of discussing risk management in the context of performance management, the survey found that less than half of the respondents reported that employees felt comfortable escalating critical risk management issues, only a third of respondents agreed that there is clear accountability for risk management failures and less than a third reported organisational support for risk management translating into sufficient funding. 40 per cent of respondents indicated that their organisation provided appropriate training/development on risk management.

Much guidance on risk management exists in published literature, standards (ISO, COSO, M_O_R etc.) and organisational documentation (e.g. JIU 2010 Review of ERM). This document is not intended to compete with those important sources of information: it is not a process manual or a comprehensive guideline on how to undertake Enterprise Risk Management (ERM). It is rather a set of proven approaches, informed by the experiences of Task Force members who have had some success in the process of integrating risk management processes into their respective organisations. The suggestions contained herein are therefore not prescriptive or mandatory and each organisation is best placed to decide on the approach suited to its own operating context and mandate.

This document should be read in conjunction with separate guidance developed by the Task Force, including the Reference Maturity Model (RMM) for risk management, and the guidelines on the preparation of a Risk Appetite Statement[1].

1.2 Reference Maturity Model for Risk Management

The HLCM endorsed the finalized RMM at its thirty-eighth session in October 2019, which identified six dimensions of risk maturity (ERM Framework and Policy, Governance and Organisational Structure, Process and Integration, Systems and Tools, Risk Capabilities, and Risk Culture) each of which could be rated against a five point maturity scale (Initial, Developing, Established, Advanced or Leading).

[1] See also Guidelines on Risk Appetite Statements CEB/2019/HLCM/26 endorsed by the HLCM at its thirty-eighth session.

The RMM recognized the importance of integrating risk management with the programme management cycle by making it an essential element for ‘Established’ risk maturity for the dimension ‘Process and Integration’.

In order to establish an organisation’s current level of risk maturity, the RMM provides a framework for evidence-based self-assessment. Through a gap analysis, organisations can then develop a roadmap to reach their target state. The approaches described in this document necessarily have dependencies on other elements from the RMM, such as culture, capacity (tools/knowledge, expertise, time), tone at the top, learning and continuous improvement.

1.3 Intended audience and assumptions

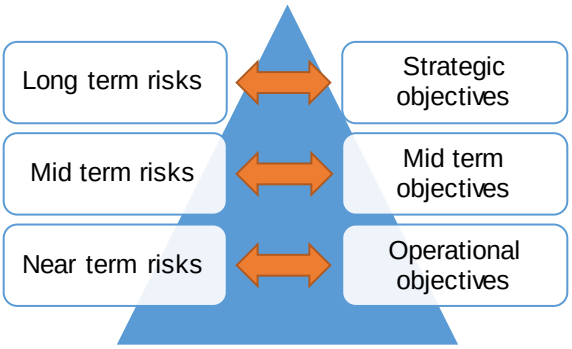
This document has been written for all staff responsible and accountable for delivery of results, including HLCM members, directors, risk specialists, results-based management (RBM) officers. It is not a technical document, but rather focuses on practical advice. It assumes that an organisation has a basic level of RBM in place and that it has already embarked on establishing the basic foundational elements of risk management best practices, such as a risk policy, a risk manual and appropriate risk governance. Generally, an organisation would need to be in the “Developing” stage of the RMM to be able to benefit from the approaches described in this document.

2. Integrate risk management with performance management processes

2.1 Establish risk assessment as an integral part of planning

Risks do not exist in isolation – in the context of UN organisations, they represent an uncertainty, which may be a threat or an opportunity to the achievement of objectives[2] typically set out under a results framework. To maximise the value from risk management, it should be linked directly to the organisation's results framework which typically reflects the highest priority elements of its mandate and mission. The planning process is often based on a set of assumptions. Assumptions that are less likely to hold as time progresses, may turn into risks. Organisations therefore need to clearly place risk management within the context of their operational activities rather than as a parallel activity. The benefits of integrating risk management with planning processes include:

Figure 1: Risk time horizon



- risks, particularly those above a specific or organisational risk appetite[3], that may affect the achievement of objectives, are identified up front and addressed by an appropriate response[4];
- risk responses can be monitored for effectiveness throughout the implementation phase and adjusted where necessary;
- the risk management process is undertaken efficiently.

TIP

Risks should be defined in the context of an objective.

Planning is a structured decision-making and resource allocation process, and for most organisations, it covers different time horizons, typically:

- **Strategic plans** may look out five years or beyond, and focus on the strategic objectives of the organisation, setting out its vision for implementation. Strategic objectives are often broad with many uncertain outcomes. The purpose of embedding risk management at the strategic planning level is to ensure that adequate attention is paid to the likelihood and potential impacts of external and contextual factors such as geopolitical threats and opportunities, changes in technology, population and migration trends, and stakeholder requirements and funding appetite.

SOME QUESTIONS TO ASK TO HELP EMBED RISKS INTO PLANNING

- Can risk information help identify which programmes/policy areas are least likely to achieve their objectives?
- Is the risk assessment timed to truly guide the planning, or is it bolted on at the end to support a pre-determined path?
- Will the organization share all available risk information with their governing body, or would it be more helpful to provide the most pertinent information only?

[2] Reference made to 'objectives' may be understood to include objectives, outcomes, targets, outputs, results or similar terms.
[3] Some organisations may choose to consider 'risk criteria' in order to evaluate the significance or importance of risks, this paper refers to 'risk appetite' which can be seen to refer to either approach.
[4] Risk response might be to avoid, reduce, share, accept or (for opportunities) pursue.

- **Programmes and budgets** usually cover periods from one to five years and outline the implementation of specific programmes with mid-term objectives and resourcing needs. Programme managers can rarely be held fully accountable for the achievement of the mid-term objectives, since time and other factors or programmes may also contribute. However, they can be held accountable to identify the risks that could affect the achievement of mid-term objectives. The purpose of embedding risk management in the programme and budget planning cycle is to encourage a dynamic dialogue with stakeholders and governing bodies who fund or jointly implement the programmes about the key factors that may jeopardize their successful implementation.
- **Projects/Work plans** are typically internal and cover the shorter-term work of individual organisational entities and staff and may be monitored with specific performance targets. The purpose of embedding risk management in the work planning cycle is to ensure that risk responses are fully reflected and resourced in implementation plans.

Embedding risk management requires a clear and iterative focus on all steps of the risk management process - identification, assessment, establishing suitable monitoring measures, and response planning. Where risk assessment can be supported and refined by data, it will be more objective and credible.

Case study 1. Integrating risk management into planning processes

"Our approach to embedding risk had both 'bottom up' and 'top down' elements. We began with annual work planning, using spreadsheet risk registers to help programmes identify and manage their own risks. This allowed the foundational learning to take place in the 'safe space' of internal meetings. Over time, as risk competencies evolved, programme plans and budgets began to take risks and proposed mitigation increasingly into consideration.

In the course of the biennial planning cycle, we reviewed our top risks for each programme, in particular those risks with clear external factors (e.g. global economic downturn), or those that the governing body could potentially influence and included these as part of the presentation of the proposed Programme and Budget, for discussion with our governing body. Over a number of planning cycles, the risk dialogue with the governing body improved significantly, and programme deliberations began to focus increasingly on addressing risks."

2.2 Monitor risks during implementation

A key aspect to embedding risk management successfully is to ensure that it is addressed iteratively during the programme management cycle. As new risks emerge, existing risks turn out to be more (or less) likely, or have different impacts than envisaged, they are reassessed and if necessary, reprioritised in terms of response. The upfront risk assessment and mitigation can be back-tested by evidential monitoring of risks to programme objectives. Monitoring of risk information may include tracking of risk indicators or oversight issues, as well as responses to actual risk incidents, both internal and external to the organisation. Objectives are not static and may evolve over time. The risks may inform the objectives and *vice versa*. It is therefore important to remain open to adapting objectives in order to adequately respond to emerging risks.

Risk appetite should act as a delegation of authority in risk taking, whether for the organisation as a whole – *vis-à-vis* its donors and other stakeholders – or internally for its executives and managers. Similar to budgeting, the process of agreeing appetite thresholds sits logically alongside the planning process, which then balances performance objectives, cost constraints and parameters for risk taking in decision-making. Breaches of risk appetite require escalation to a higher level of management and may require a formal waiver or risk acceptance at the higher level of authority.

Risk appetite may be established to support management action triggers tied to risk monitoring. Breaches of appetite may also form the basis for internal escalation and to external stakeholders. If using a traffic light system (red-amber-green), where risks are deemed 'amber', this should trigger a discussion with, for example, a functional specialist as to whether action or reassessment is necessary. Where risks are deemed 'red', mitigating action and identification of a 'path to amber or green' should be mandatory. This process of risk monitoring is more interactive and regular than assessment processes linked to periodic planning, and it brings the risk management process to life. It reinforces risk ownership and drives a continual process of readjustment and fine-tuning of plans, whether at the strategic, programme and budget, or work planning level.

Some risk monitoring measures may be common across the organisation and determined 'top down', but it is often more useful for managers who are responsible for specific programmes and especially at the work planning level to determine their own monitoring measures and agree suitable risk appetite thresholds with their internal management.

Case study 2. Responding to emergencies outside of the planning process

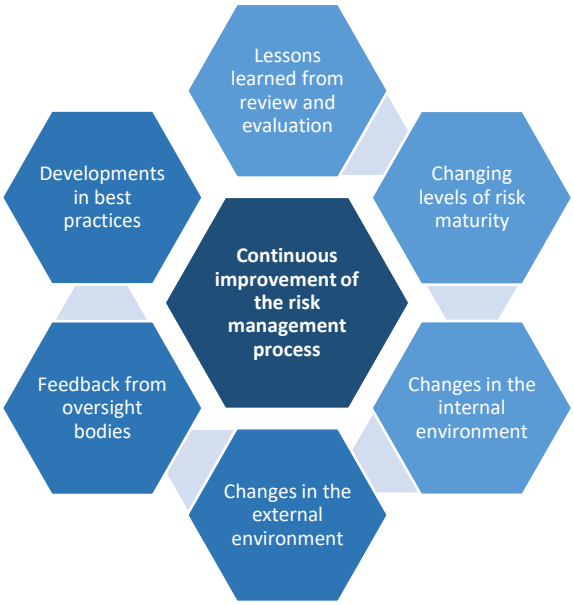
"As a large humanitarian organisation we have a longer-term planning process and engagement with key stakeholders, but this may not foresee sufficient funding for a sudden onset emergency. Our emergency preparedness and response capability is therefore central to our ongoing resource planning. We continually monitor and assess risks to vulnerable populations and where a new crisis occurs or is seen to be developing, we alert donors and revise budgets. If the crisis exceeds the country office's ability to respond, then it is elevated to ensure that regional and/or global support is provided."

2.3 Harness feedback and continuous improvement

Post-implementation, many organisations have a process to review and evaluate the effectiveness of their strategic and programmatic planning. This process considers the management of risk throughout the planning and implementation cycle so that lessons learned are properly captured, disseminated and applied to future planning activities. The review and evaluation of the previous implementation period may help identify recurring or similar risks for the upcoming period. Some organisations report back to governing bodies or management on the actual occurrence of risk events, whether the risk response was effective or relevant in order to re-use effective measures and reconsider those that were less effective.

This process of feedback and continuous improvement can also be applied to the risk management process itself. As Figure 2 shows, a number of different sources of information and change can drive the need to adjust and improve risk management processes to ensure that they remain applicable and fit for purpose in the organisation.

Figure 2: Driving continuous improvement in risk management maturity



As the organisation increases its overall risk maturity and moves along the maturity levels set out in the RMM, aspects of the risk management processes that were suitable for a less risk mature organisation may need revision and update. Similarly, changes to either the internal environment (such as the introduction of new systems or processes) or the external environment (such as shifting attitudes of donors or new mandates from Member States) may also require refinements to risk management processes. The model for an organisation's risk management maturity is not expected to be static, but should be dynamic, absorbing and integrating best practices and lessons learned both from internal experience as well as external factors as international standards and stakeholder expectations evolve.

Case study 3. Feedback and improvement of risk registers

"Our organisation has over 160 different risk registers from field operations and headquarters entities. In 2018, for the first time we had sufficient risk management resources to systematically review all risk registers. As part of this review, we provided detailed feedback to risk owners to improve the quality of the risk registers. This process was instrumental in enhancing the quality and effectiveness of risk management in the field and allowed us to analyse overall risk data and draw conclusions from it in support of organisational decision-making and prioritisation.

Another outcome from the review was that we identified a number of strengths and weaknesses in how risk management was being applied across the organisation. We used this information to update our risk register tool and develop frequently asked questions to be circulated to all staff completing risk registers. Examples of changes introduced included:

- *Allowing specific individuals to be assigned responsibility for particular treatments in the risk register tool to enhance and clarify accountability;*
- *Creating a report that allowed risk managers to automatically generate a work-plan for outstanding risk treatments from the risk register tool to support planning; and*
- *Generating automatic reminders when outstanding treatments were due for completion to make risk management an ongoing process rather than a once a year exercise.*

These minor changes enabled us to adjust and enhance our risk management processes and tools, keeping them relevant to the organisation."

3. Operationalize risk management through enablers

The following section outlines enablers identified by UN agencies as potentially useful to ensure that risk management takes root in an organisation's reflexes. As per the introduction, the guidance that follows is not prescriptive; however, it is likely to help embed risk management.

3.1 Combine formal and informal mechanisms

Organisations may want to establish both formal and informal mechanisms to encourage the engagement of all staff in risk management activities. *"Formal mechanisms provide a tangible management structure, while informal mechanisms help people to accept, understand and operate, and refine the tangible management structure."*[5]

The blend of both mechanisms will depend on the external environment in which the organisation operates, and on internal factors, such as the existing risk culture, strategic objectives, and risk appetite. To improve the effectiveness, formal and informal mechanisms should work together in a complementary manner.

Some common formal mechanisms are the endorsement of a risk management policy, the definition of a risk appetite statement, establishment of clear governance structure (e.g. Three Lines of Defence[6]), risk register and reports, and risk committees, among others. Formal mechanisms may also include aligning risk with the operating model and establishing a risk management process that is centred around protecting the value of the organisation. It may be useful to communicate that value is created, preserved, or eroded by management decisions in all activities, from setting strategy, allocating resources and operating the organisation day-to-day, thereby emphasizing the need for risk management to be an ever-present consideration in decision-making.

To achieve a stronger linkage between decision-making and risk management, organisations may want to consider the implementation of a more integrated governance structure. This structure should facilitate and encourage the cooperation and communication of all the actors involved in the enterprise performance and risk management.

This visible and evidential structure should also be reinforced by informal mechanisms. Some common examples of informal mechanisms would be risk facilitation by internal risk coordinators, one-to-one meetings with risk focal points, mentoring and training sessions, risk forums and workshops, and a clear "tone at the top" that is promoted by senior management.

The self-reinforcing blend of both informal and formal mechanisms should also be considered when designing and establishing an effective risk communication structure. This might include formal risk committees, timely dissemination of risk information, tailored reporting for each audience, as well as informal meetings between different functional disciplines to encourage open and transparent discussion of shared risks. These interactive and informal processes for communication help to build participation and commitment to addressing risks.

[5] The Association of Chartered Certified Accountants (ACCA) Risk and performance: Embedding risk management
[6] An industry model explained in The Institute of Internal Auditors position paper of January 2013.

Organisations may also consider embedding risk management in existing forums for decision-making, as opposed to establishing separate committees or formal structures that would focus on risk management in isolation. Including risk management as a specific agenda item in existing forums such as executive management meetings, strategic planning, corporate reviews and statutory monitoring, as well as operational briefings, can assist with alignment and encouraging true ownership of risks.

- Build cumulatively, with measured and steady momentum.
- Show managers what's in it for them, and the organisation.
- Encourage true end-to-end ownership of risks.

3.2 Strengthen risk capabilities

Although managing risks may be something that managers may feel they are already doing intuitively, there may be many organisational inconsistencies reflecting the different skills and experience amongst managers. In this regard, risk management is a topic that many people may struggle to visualize and articulate conceptually, but they may find it easier to apply in a real life situation. (see also 2.2 Monitor risks during implementation).

Risk management, and its associated policies and procedures may appear administrative in nature. A critical success factor in embedding risk management is demonstrating its practical application and benefits in contributing to increasing the probability of achieving results. Some examples for how to do this can include:

i) Engage with management directly in team meetings, use hands-on practical examples, to help programmes with their risk related discussions. When undertaking risk identification and assessment, focus on the substantive content of the work and the results to be achieved, rather than the process itself. Involve and solicit inputs from the experts through discussion and facilitation in identifying, assessing and responding to risks that jeopardize the achievement of their objectives.

ii) Use peers from within the organisation, who may be more mature in risk management to provide examples of success and failure stories and share experiences with other programme staff. (see also 3.3 Build a network of risk ambassadors)

Involve managers from the outset of the risk journey, before there is too much risk machinery (policies, processes, etc.), and encourage them to continue to persevere and focus on risks. As practiced with change management, the payback from early engagement is high and managers will understand that preventing a risk at the outset is much easier than trying to deal with it afterwards.

Whatever the hierarchical level of risk management, the active involvement of stakeholders will help embed the process. The discussion often encourages the definition of priorities and support strategic resource decisions and trade-offs.

In particular, for the governing body approved planning, Member States and donors should be actively involved in confirming the risks, risk appetite and high-level mitigation approaches in the context of the objective they endanger, including identification of the risk event and the possible cause.

Case study 4. Changing the methodology to help make risk management a reflex

"For several years Country Offices have been required to keep a risk register and update this along with their six-monthly annual planning reviews. However, many of the risks they captured were quite high level – external and contextual risks where their ability to mitigate locally was limited. For many countries the exercise had become something of a 'form filling' exercise providing HQ with what the Country Offices thought they wanted.

To help bring the process to life, a new risk categorisation was introduced, covering all the core functional specialisms so that countries would give equal focus to their internal and controllable risks as those that were outside their control. The assessment methodology also helped them to distinguish between more frequent risks that they needed to manage every day, versus rarer risk events for which they may need to consider their response planning more carefully.

We are still working with countries to improve the quality and consistency of their risk assessments and mitigation planning. We do rely on core HQ functions and our regional bureaux to provide constructive review. For higher risk countries we will often directly support the planning review cycle and facilitate the process".

3.3 Build a network of risk ambassadors

Organisations may identify and train risk management focal points to take the risk message forward, using the established train-the-trainer approach. In addition to providing more capacity, this will ensure better and more focused risk identification/ assessment/ treatment, as programme staff will typically be closer to the subject matter of the programme.

When scaling up or rolling out risk management throughout an organisation, it may therefore be helpful to create such a network of decentralized risk management experts, which will help:

- Provide sufficient support and coordination across the organisation for risk management activities to be performed in a consistent and technically robust manner;
- Ensure a multi-functional team approach in risk assessment and treatment;
- Prepare and deliver training of risk management trainer programmes;
- Reinforce ownership of risks at the level of programme staff and provide the required autonomy to focus on the key risks in the given location and/or subject area;
- Help to define and monitor appropriate risk appetite metrics in consultation with risk owners; and
- Strengthen the message that risk management is a substance-driven need and the exercise is intended to achieve more effective and reliable achievement of objectives.

Acknowledge a proactive and results-oriented focus on risk management through positive reinforcement.

Case study 5. Introducing a major new time-bound initiative to embed risk management in the field and transform the organisation's risk culture

"An important part of the initiative was creating a number of senior level positions in high risk field operations to act as dedicated risk advisors to the senior management of the operation.

The risk advisors are embedded alongside the first line of defence although to maintain a degree of independence and strategic overview they were not appointed in management or supervisory roles. Instead they work across all functional areas to help identify existing risks, anticipate emerging risks, and design, implement and monitor appropriate preventive measures and responses to key risks. The risk advisors also work with relevant external stakeholders including donors and governments to ensure that risk management is inclusive and transparent. They also train colleagues and partners to raise awareness and improve risk management literacy and skills. The ERM team at headquarters coordinates a global network of risk advisors to share good practices and lessons learned across operations and regions.

The ultimate goal is that once this injection of risk management expertise and attention has been made into an operation, it will eventually become mainstreamed and self-sustaining such that the risk advisor role may no longer be required."

3.4 Focus on user experience and value add

Although risk management is about the substance, ineffective processes or tools can inhibit risk management from being effectively institutionalised. If operational staff feel the risk process is cumbersome or frustrating, they may be reluctant to engage. Therefore, developing integrated processes, systems and tools that enable the operational teams to feel empowered and in control of their risks will support embedding risk into the organisation.

i) Choose a risk repository (whether a tailor made solution or simply spreadsheets) appropriate to the scale, complexity and maturity of the organisation keeping it intuitive and simple. Centralized data input, good quality reporting with easy access, user-friendly tools, can all help reduce the perception of risk management being an administrative burden. Listening to users' concerns and addressing them openly and pragmatically will be appreciated by stakeholders.

ii) Centralized data quality assurance can strengthen credibility of data, and in turn, reinforce the use of data for decision-making and reporting.

iii) Early engagement from functional specialists will also help to improve the quality of discussion and consistency of risk assessments and mitigation plans. It will also encourage the organisation to continuously learn from its mistakes and build institutional knowledge in its areas of functional expertise.

Case study 6. Organising risk workshops to raise the awareness of risk management in specific units

"One of the main problems in our risk management system was the disconnection existing between the "policy units" and the "management unit".

The risk coordination function was in charge of the update of the risk register and the overall coordination of the risk actions, based on feedback from risk owners and risk focal points. However, staff in policy units had little awareness of the recently implemented risk policy, and the participation rate had room for improvement.

To increase the awareness of the importance of a well-functioning risk management system, the risk coordination function led different workshops targeting middle managers of specific policy units. The workshops were based on the extended enterprise model and invited units to brainstorm about their core business, inputs, outputs and external environment. After this reflection, they had to identify all the risks associated to these elements and prioritise them by criticality.

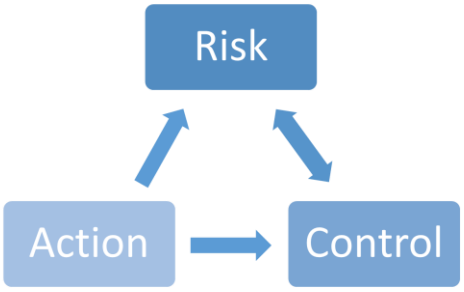
After the workshop, the risk coordinator sent a sub risk register to the unit leader based on the discussion, inviting them to keep working on the potential risks and mitigation actions. At the same time, with the gathered insights, the risk coordinator complemented the information of the organisation's risk register.

The overall exercise served to enhance the relevance of risk management at all levels of the organisation and to raise the awareness of the existing policy. It also helped motivating staff and managers to think about their own business and associated risks, an exercise that is difficult considering teams' workload and administrative responsibilities.

The main results were reflected in the rate of participation during the update process and positive feedback coming from different participants."

3.5 Reinforce the link between internal controls and risks

Figure 3: Relationship between risks, actions and controls



Internal controls, risks and actions (risk responses) have a three way relationship (Figure 3):

- Risks may be addressed by controls and actions
- Effective controls mitigate risks
- Actions may target risks (to reduce risk exposure) or controls (to address a control gap)

By linking these three variables, and in particular by demonstrating the relationship between risks and controls they can be mutually supportive processes. Internal controls are recurring mitigation actions that an organization undertakes to reduce the likelihood of an unfavourable event occurring, or the impact if it does. Control assessments are typically undertaken based on predefined criteria to determine the effectiveness of the control on mitigating the risk.

Many organisations have a control framework, and in some organisations the ownership of risk management and controls is consolidated. Strengthening the internal control framework is an initiative almost universally recommended by auditors, and will also provide greater assurance to management that the control environment is robust.

While a small organisation could attempt to link controls and risks manually, typically established maturity organisations would use an integrated ERM system that offers risk, control and action functionality.

Strengthening the links between internal controls and risk management through, inter alia,

i) targeted use of controls to mitigate risks – controls can be re-used on other risks;

ii) identifying critical control gaps through risk analysis and addressing these; and

iii) optimizing controls (and hence reducing risk) in business processes, especially upstream processes and programme design.

Case study 7. Strengthening the relationship between the internal control effectiveness and residual risk assessment

"In our fraud risk assessment exercise, we calculated the residual fraud risk based on the relationship between the "inherent risk" and the "control effectiveness." If the inherent risk is "high" a control effectiveness of "effective" reduced the residual risk to "low", however, assessed as "not effective" the residual risk remained high. In the context of over 130 country assessments, one of the challenges faced was regarding the objectivity of the "control effectiveness". It was perceived as possible that country offices were over-estimating their control effectiveness in order to achieve a fraud risk assessment of 'low'.

Therefore, to bring more objectivity in the risk assessment, we developed a list of general questions for different types of "effectiveness" and the "net effectiveness" used to be calculated automatically based on the answers provided for each question and thereby calculating the residual risk automatically. The net effectiveness was based on various tailored weighted control assessment criteria, depending on the type of control.

This approach was found to be a useful mechanism to bring more objectivity thus enhancing the quality of the assessment. Looking at continuous improvement, we then creating a list of standard mitigation items (based on the questions) to allow the country offices to develop action plans for fraud risks using standard mitigation items."

3.6 Consider risks as potential opportunities

Consider "positive risks", or opportunities – and how to exploit them. Viewing risk as having only a negative effect can lead to the organisation being underprepared for opportunities, and failing to deliver other priorities (e.g. innovating, improving service provided to stakeholders and process streamlining). Organisations must pursue risk to survive and prosper. If opportunities are considered when defining strategy, those risks (positive or negative) can actually drive the strategy setting. (see also *Strategic plans* under 2.1 Establish risk assessment as an integral part of planning).

Organisations naturally assume strategic and business risks as part of their mandate and their issue may be their capacity to continue to absorb risk. This can be a positive discussion around the business model: where are the areas that make the most sense for the organisation to focus its efforts and resources?

Case study 8. Thinking of risks as potential opportunities

"Risk is often defined as the probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities. However, consider risks as a variation around an expected outcome, and the event may cause the outcome to be worse or better than expected.

In our agency, one of the donors was contributing about 15 per cent of our total funding base, and the agency was heavily dependent on its contribution. Due to changes in the government and some conflict between the agency mandate and incoming government election manifesto, the donor decided to stop funding the agency and thereby to put consistency of resource mobilization at risk. The agency took that as a challenge and prepared an extensive mitigation plan to counter the budget deficit. The plan included a significant advocacy campaign to highlight the funding shortage and the potential effect on its mandate. The agency used social media and other communication channels to reach out to many small donors thereby broadening the donor base. The agency also used other mitigation actions to promote its status as a highly accountable organisation. Due to these efforts, the agency was not only able to fill the 15 per cent gap created by that donor but surpassed the prior year in terms of resource mobilization, thereby converting a potential risk into an opportunity."

3.7 Focus on new and emerging risks

Many organisations have implemented risk assessment and monitoring processes around their existing activities, but few have applied the same discipline and effort around new and emerging risks, where decisions often have the greatest impact. New or significantly expanded programmes and major internal change initiatives usually require much more input and risk expertise to achieve smooth implementation. If the full risk discussion only happens after the decision has been made, its relevance is relegated to 'scorekeeper', or worse, 'undertaker' if the initiative struggles! Risk assessment therefore needs to happen upfront, not after the fact, to be truly integrated with planning and decision-making.

This is an important area of risk culture and 'tone at the top'. The organisation will follow senior management's lead if they visibly apply risk management approaches to major policy setting and change initiatives. Where this happens, the organisation will see that risk management is not just something to be applied to core functions and business as usual, but instead something that is embraced for all key activities because it adds value and contributes to the achievement of objectives.

Conducting a risk assessment of any policy change or other change initiative at an early stage (and periodically refreshing it) can identify potential pitfalls to be avoided or opportunities to be exploited. The assessment can also help identify strategies to maximize the chances of success that might not otherwise have been pursued.

3.8 Apply risk data to support change initiatives

Risk data can support and inform the development of change initiatives such as new or revised policies, systems, processes, or organisational restructuring in two key ways. Firstly, risk data can feed into decision-making to determine which change initiatives to launch in an organisation. For example, analysis of significant risk events that have materialized may identify a recurring root cause that could be addressed by updating relevant policies and processes. In such a case, this change could be prioritised in order to more effectively manage significant risks and their root causes. Conversely, where an area is assessed consistently as being of low risk, an organisation may question whether the time and cost required to establish a policy governing it is commensurate with the benefit gained from its development, since weaknesses in this area have been assessed to have minimal impact.

Secondly, risk data can also inform the management of change initiatives, increasing their chances of success. Using a risk lens, asking questions such as those below can help change initiatives be as effective as possible.

- What could impede the initiative achieving its objectives and what actions and resources would be required to reduce the chance that the negative event occurs?
- What monitoring techniques can be used to understand whether the project is on track, in particular in consideration of changing external factors?
- How can the intended impact be measured, and what factors might influence the reliability of that measurement?

In addition to actively managing risks to delivering the change, risk data (such as analysis of risks and issues from previous or similar change initiatives) can also inform the implementation approach of other upcoming initiatives.

Case study 9. Using risk data to drive change

"In our field-based organisation, a few years ago a fraud risk materialized resulting in harm to beneficiaries and negative impact on our reputation. Following this, risk managers and the team on the ground worked to identify the root causes that had enabled the risk to materialise. One of these key root causes was that there was no easily accessible feedback mechanism for beneficiaries to report concerns in their own language, at a convenient time, in a safe manner. The team introduced a series of change initiatives to address these gaps, including the establishment of a confidential call centre.

We subsequently identified a number of other operations that faced similar fraud risks. Through our network of risk managers, we were able to take the change initiatives introduced in the first operation and apply them to these other operations. This meant that we used risk data from one operation (specifically information on what mitigation activities worked) to proactively reduce the likelihood of the same risk materialising in other locations."

3.9 Strengthen risk culture

Ultimately, the maturity of an organisation's risk culture is evident in its ability to link risk management to decision-making, performance and learning. Embedding a robust risk culture throughout the organisation requires establishing and communicating desired behaviours. Demonstration of it by senior management – "tone and commitment from the top" – alone may not ensure staff undertake good risk-based decisions. However, it is the visible actions that matter most.

Just as organisations undertake to establish and embed core values (principles and beliefs) and competencies (knowledge, skills and abilities), senior management also need their staff to understand the importance of risk culture to support their performance objectives. Managers need to communicate clearly and consistently with their staff about identifying and responding to risks and opportunities they face in their day-to-day work which may impact the achievement of their planned goals.

Staff are also more likely to be highly motivated to perform well when they see a clear path to career growth and development where their risk-awareness is recognised. Risk accountability can be used as an instrument to align individual culture and performance and the ability to factor risk management into day-to-day decision-making in operations should be a core aspect of all individual performance management processes.

Lastly, external stakeholders expect a productive and transparent risk and performance culture to be embedded across the organisation. It provides assurance that their investment is well managed and their chances of achieving defined objectives optimised.