Enterprise Risk Management and Internal Control Framework

A Guide for Managers

August 2021
Table of Contents

I. BACKGROUND 3

II. PURPOSE 3

III. DEFINITION 4

IV. ENTERPRISE RISK MANAGEMENT PROCESS 5
   IV.1 Establishing the Context 6
   IV.2 Consideration of Risks and Objectives 8
   IV.3 Event Identification and Risk Assessment 12
   IV.4 Risk Response and Internal Control Activities 19
   IV.5 Information and Communication 23
   IV.6 Monitoring and Assurance 29

V. RISK GOVERNANCE, ROLES AND RESPONSIBILITIES 30

ANNEXES 38


Annex 2. Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control Effectiveness 40

Annex 3. Glossary of Terms and Definitions 42

Annex 4. Risk Assessment Interview Sample Questionnaire 44

Annex 5. Local Risk Management Committee Generic Terms of Reference 46

Annex 6. Annual Enterprise Risk Management Reporting Template 47
<table>
<thead>
<tr>
<th>Document date</th>
<th>Description of Change</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021-08-24</td>
<td>- Adding information regarding the Risk Treatment and Response Plan Progress Scorecard</td>
<td>25 -27</td>
</tr>
<tr>
<td>2021-02-02</td>
<td>- Clarification on the reporting modalities: update to paragraph (ii).</td>
<td>25</td>
</tr>
<tr>
<td>2021-01-13</td>
<td>- It explained that the Residual risk is calculated by subtracting the Level of Internal Control off of the Risk Exposure and that it should be expressed as a number between -5 and 5, but it should be a number between 4 and 4. - Typo in third paragraph of the Internal Controls. With regard to the identified risks, comprehensive Risk Treatment and Response Plans shall outline the main controls that management that has already established...</td>
<td>12; 19</td>
</tr>
<tr>
<td>2020-12-15</td>
<td>- A more detailed Risk Governance Structure, Change in Reporting Modalities and a new annual Enterprise Risk Management Reporting Template</td>
<td>28; 22,45</td>
</tr>
<tr>
<td>2020-07-28</td>
<td>- Risk universe and taxonomy - The Risk Governance Structure - The relation between ERM and Internal Control - Risk reporting and frequency</td>
<td>7; 28; 22</td>
</tr>
</tbody>
</table>
Enterprise Risk Management and Internal Control

A Guide for Managers

I. Background

Enterprise Risk Management (ERM) facilitates effective strategic decision making in a modern organization. It fosters healthy dialogue at the most senior managerial level on the critical matters the United Nations is facing in an environment of growing complexity and uncertainty. It supports enhanced accountability and contributes to the implementation of a best practice governance framework, through the transparent prioritization and clear ownership of objectives, risks, and managerial responses.

The implementation of the Secretariat-wide ERM and Internal Control framework is guided by the following documents:

(i) **Policy** document outlining the purpose, governance mechanisms and principles that guide the adoption of ERM in the Organization. It was formally approved by the Management Committee in May 2011 and presented to the General Assembly in March 2012.

(ii) **ERM Guide for Managers**, describing the Methodology and concrete steps for implementing ERM across the Secretariat.

II. Purpose

The main purpose of this Guide is to lay out clearly each step of ERM implementation for the practitioner to follow along. The Guide is divided into three sections: the first part is devoted to definitions of risk and ERM. The second part introduces the ERM framework which provides functional structure for implementing the ERM process. And the last part focuses on risk governance that includes the way in which ERM roles and responsibilities are divided in the organizational structure.

A consistent ERM framework with a Secretariat-wide scope and a robust, yet practical governance structure are essential to ensure the alignment in the understanding of objectives and related risks at different levels of the Organization and with Governing Bodies, as it promotes transparency and facilitates open discussions on strategic issues, enhancing stakeholders’ confidence.

The Secretariat-wide ERM process provides management with the necessary tools to fully understand the root causes of a risk, make results across the Secretariat comparable and design proper response strategies. Prioritizing the response on critical risk areas, it progressively contributes to informing the strategic planning and resource allocation process, enabling senior managers to make better, properly informed decisions.

"One of the greatest contributions of risk managers – arguably the single greatest – is just carrying a torch around and providing transparency” An ERM Officer
III. Definition

Consistent with the best international standards risk is defined as an “an effect of uncertainty on objectives”. Effect is generally thought of as a deviation from expected. It can be positive, negative or both, and address, create or result in opportunities and threats.

ERM, on the other hand, is a structured process. It is defined as:

"The process of coordinated activities designed to direct and control an organization with regard to risk, the effect of uncertainty on objectives. It is effected by governing bodies, management and other personnel, and applied in strategy-setting throughout the Organization”.

Accordingly, an effective system of internal control is encompassed within and is an integral part of enterprise risk management. Enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualisation and tool for management.

ERM addresses the strategic, governance and financial risks associated with the execution of the mandates and objectives as defined by the Charter of the United Nations, as well as the operational risks inherent in the daily operations that support the achievement of those mandates.

Implementation of the ERM with a balanced focus among all risk categories enhances the governance and management practices of the Organization, as outlined below:

(i) **Focus on Objectives** – Increased effectiveness in the achievement of the defined objectives and mandates through a consistent identification, assessment, and management of risks among Secretariat entities.

(ii) **Internal Controls** – Embedded risk and internal control management activities, enabling risk management to become an integral part of the processes and operations of the entire Organization, and determining the type of risk mitigation or corrective measures necessary to manage the identified risks.

(iii) **Efficient Use of Resources** – Improved performance against objectives, contributing to reduced waste and fraud, better value for money, and a significantly more efficient use of available resources.

(iv) **Accountability** – Enhanced accountability and performance management through the definition of clear risk management roles and responsibilities.

(v) **Results Based Management** – Promotion of a risk driven culture through a more informed risk based decision-making capability, as the significance of risks and the effectiveness of designed controls are explicitly considered when evaluating programmes and relevant budget allocations, according to an effective results-based management approach.

---

(vi) **Transparency** – Improved transparency within the Organization and towards member states, as risks are clearly communicated internally and externally through periodic formal reporting by management to the Independent Audit Advisory Committee (IAAC) and the General Assembly.

(vii) **Assurance** – Improved assurance over internal controls through the formal recognition of management’s responsibility for effective controls, and the appropriate management of risks.

(viii) **Oversight** – The ability to enhance governance and oversight functions.

(ix) **Governance** – An increased capability of senior management and governing bodies to make informed decisions regarding risk/reward trade-offs related to existing and new programmes, through the adoption of a structured approach for the identification of opportunities to enhance the allocation of resources throughout the Organization and reduce related costs.

**IV. Enterprise Risk Management process**

ERM is a continuous, evolving and integrated process owned and executed by management. ERM is not a periodic validation exercise, it evolves over time in accordance with the pace and scope of the changes, and it integrates with other UN Entities with the objective of merging both risk and return information into strategic planning and decision making. The ultimate goal of this process is to make the ERM a part of the Organization’s culture.

The main components of the risk management process cycle are illustrated in Figure 1 below, and further described in this section of the document. This cycle steps operate within the functional ERM framework structure. The definition of all the relevant terms is included in Annex 3 of this document – Glossary of Terms and Definitions.

**Figure 1- Enterprise Risk Management Process Cycle**
In particular:

(1) **Establishing the Context** – Establishing the context encompasses the definition of the Organization’s overall risk management approach, as outlined by the Policy articulating the purpose, governance mechanisms, and principles that guide the adoption of the framework.

(2) **Consideration of Risks and Objectives** – Risks are mapped and aligned to objectives, mandates and strategic initiatives at both the UN Secretariat and entity level. Specific measurement criteria for risk evaluation are also defined.

(3) **Event Identification and Risk Assessment** – Risks are assessed in the context of the objectives, mandates and strategic plans through interviews, risk questionnaires, workshops with relevant management and staff, and other sources. The analysis of trends in recommendations from oversight bodies could also provide important indications. Identified risks are then measured and scored according to the perceived impact, likelihood and level of managerial and internal control effectiveness.

(4) **Risk Response** – Risks are prioritised based on the overall ratings for each risk in terms of risk exposure and then, through the consideration of the level of risk mitigation and internal control effectiveness, in terms of *residual risk*. Appropriate risk treatments are determined based on the overall risk prioritisation and implemented according to defined timelines and responsibilities. An effective system of internal control is an integral part of enterprise risk management.

(5) **Information and Communication** – Ongoing reporting on results of risk assessments, including risk treatment plans and actions, is established. Appropriate communication and training programs are developed across the Organization to nurture the development of a sound risk aware culture and build adequate capacity and critical skills.

(6) **Monitoring and Assurance** – Ongoing monitoring of risks and internal controls are implemented.

A detailed description of the specific steps to be followed in the implementation of an effective enterprise risk management and internal control framework is provided below.

### IV.1 Establishing the Context

In order to provide direction to the process of implementation of the ERM framework, the Organization has adopted an overall Enterprise Risk Management and Internal Control Policy, articulating the principles that guide the adoption of the framework, both at the Secretariat-wide and at the entity level.

**Principles**

The ERM and internal control framework is guided by the following core principles:

(i) **Embedding** – Risk management must be explicitly embedded in existing processes. Appropriate flexibility needs to be applied in the execution of strategies
and allocation of relevant resources through the proper consideration of the risks that could affect the achievement of the objectives applicable to each entity, and the overall Secretariat.

(ii) **Consistency** – The Organization shall adopt, as part of its decision-making process, a consistent method for the identification, assessment, mitigation, monitoring and communication of risks associated with any of its processes and functions, in an effort to efficiently and effectively achieve its objectives.

(iii) **Integration** – The ERM and internal control framework must be fully integrated with the major operational processes, as strategic planning, operational and financial management, and performance measurement and management. Risk management shall be integrated with the adoption of an effective results-based management approach. ERM complements results-based management by enabling to effectively achieve set objectives with a clear, shared understanding of the internal and external uncertainties that may impact activities. High priority risks and the effectiveness of related controls shall also be fully considered in the evaluation of programmes and relevant budget allocations.

The effective implementation of the framework within the Secretariat relies as well on:

(iv) **Management Ownership** – Risk owners and management across the Organization must have a sound understanding of the risks impacting their operations, and the level of flexibility provided to appropriately determine the available and appropriate course of action to manage those risks, increasing accountability.

(v) **Risk Aware Culture** – A risk-focused and results-oriented culture shall be nurtured, moving the Organization from the current predominantly risk averse culture, where the focus is merely on risk avoidance, to a risk aware culture, where decisions are driven by a systematic assessment of risks and rewards. The dissemination of information and best practices regarding risk and internal control management principles shall be supported across the Organization, developing appropriate communication and training programs.

(vi) **Communication** – Adequate information shall be provided to senior management, the Management Committee, the Secretary-General and the General Assembly. The governing body, with the advice of the Advisory Committee on Administrative and Budgetary Questions and the Independent Audit Advisory Committee, will be then in a position to effectively fulfil its responsibilities of provision of governance and oversight, and to take decisions on the acceptance of proposed modifications or enhancements of the internal control system.

**Commitments**

The strong support and commitment of the General Assembly, the Secretary-General and senior management are essential for the establishment of effective risk and internal control management processes. A sustainable framework is therefore based on:

(i) **Support** – The endorsement and consistent support from senior management, confirmed by visible actions, is critical for the successful implementation of the framework.
(ii) **Accountability** – The adoption of an effective framework relies on the full ownership and accountability of management at all levels throughout the Organization for risk management and internal control activities.

(iii) **Resources** – Risk and internal control management shall be supported by adequate resources at the entity level.

**IV.2 Consideration of Risks and Objectives**

"If one does not know to which port one is sailing, no wind is favourable" Seneca

**IV.2.1 Tailored Risk Catalogue**

The initial stages of the risk assessment process require the alignment and mapping of risks to the underlying strategies, plans and objectives, based on the Secretariat’s **Risk Universe**. The updated Risk Universe, attached to this Guide as Annex 1, presents a high-level description of all the risks relevant to the Organization, and shall be tailored, as required, to reflect the profile of the organizational unit under consideration. Based primarily on its mandates and objectives, as well as its strategies and operations, each entity shall develop its own risk catalogue as a sub-set of the UN Secretariat Risk Universe, so that eventually, all risks identified within the Organization, at each organizational or functional unit level, shall be traced back to the corporate-level Risk Universe. It might be worthwhile to note that although the risk universe is comprehensive, it might not be exhaustive, as new and emerging risks could arise.

Through a common taxonomy of risks and an agreed set of definitions, the Organization adopts a common risk language, and becomes able to collect and appraise risk information on multiple levels across the entire Organization and evaluate it in a consistent and integrated manner. Through this process, the Secretariat will also be able to understand the impact of various alternate response strategies on an organization-wide basis, as well as to assess the overall effectiveness of existing internal controls and measures of risk mitigation.

The tailored **Risk Catalogue** at department and office level should be based on the experience of the department or office. In this perspective, process flow analyses, incident reports, the results of previous risk assessments, and a detailed *analysis of trends and common areas in past recommendations of oversight bodies* could provide extremely valuable indications. The consideration of anticipated future activities could also provide very useful indications.

In order to be able to accurately reflect the operations of each entity, the definition of the entity-level risk catalogue based on the Secretariat-wide risk taxonomy should allow some degree of flexibility. Where needed, entity-specific risks could be created under the relevant risk categories, or existing risks could be divided in specific sub risks.
Example

Customization of the entity-level risk catalogue

The entity-level risk catalogue could be tailored to the specific risks identified at department or office level through the creation of sub-risk areas, e.g., regarding peacekeeping operations, sub-dividing the 'Air, Land and Sea Operations' risks as follows:

3.3.8 - Air, Land and Sea Operations  ➔  3.3.8.1 - Air Operations
3.3.8.2 - Land Operations
3.3.8.3 - Sea Operations

The Risk Universe of the Secretariat identifies and defines a catalogue of 134 risks, categorized into seven major risk areas: (1) Strategic, (2) Governance, (3) Managerial, (4) Operational, (5) Financial, (6) Compliance, and (7) Fraud and Corruption risks. The definition of each risk is provided in the Risk Catalogue that complements this Guide.
Following the definition of the objectives and scope of the risk assessment, the scoring criteria for the measurement of risks shall be determined. According to best practice, risks will be measured in terms of:

(i) **Impact** – The result or effect of an event.

(ii) **Likelihood** – The possibility that a given event will occur.

(iii) **Level of Internal Control / Management Effectiveness** – The perceived effectiveness of the internal controls, processes and activities in place to manage or mitigate a risk. In this context, internal controls are defined as the processes, effected by an entity’s governing body, management and other personnel, designed to provide reasonable assurance regarding the achievement of its set objectives.

The Organization has defined the scoring criteria for the measurement of impact, likelihood and level of control effectiveness in mitigating risk at the Secretariat and entity level, as described in Annex 2 of this Guide. Where applicable, the common criteria shall be *tailored* by each entity to their risk profile and operations. For example, the absolute terms of the potential financial impact should be adjusted to the size of the entity’s budget, or the description of the organizational scope should be tailored to the entity’s specific governance and structure.
### Figure 3 – Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control / Management Effectiveness (Annex 2)

#### Impact

<table>
<thead>
<tr>
<th>Score</th>
<th>Rating</th>
<th>Safety and security</th>
<th>Duration</th>
<th>Organizational and operational scope</th>
<th>Reputational impact</th>
<th>Impact on operations</th>
<th>Financial Impact (measured in terms of budget)</th>
<th>Required action to recover</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Critical</td>
<td>Loss of life (staff, partners, general population)</td>
<td>Potentially irrecoverable impact</td>
<td>Organization-wide inability to continue normal business operations across the Organization</td>
<td>Reports in key international media for more than one week</td>
<td>Inability to perform mission or operations for more than one month</td>
<td>&gt;5 per cent &gt;$500 million</td>
<td>Requires significant attention and intervention from General Assembly and Member States</td>
</tr>
<tr>
<td>4</td>
<td>Significant</td>
<td>Loss of life due to accidents/ non-hostile activities</td>
<td>Recoverable in the long term (i.e., 24-36 months)</td>
<td>Two (2) or more departments/offices or locations: significant, ongoing interruptions to business operations within 2 or more departments/ offices or locations</td>
<td>Comments in international media/forum</td>
<td>Disruption in operations for one week or longer</td>
<td>3-6 per cent $300 million-$600 million</td>
<td>Requires attention from senior management</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
<td>Injury to United Nations staff, partners and general population</td>
<td>Recoverable in the short term (i.e., 12-24 months)</td>
<td>One (1) or more departments/offices or locations: limited impact within one or more departments/offices or locations</td>
<td>Several external comments within a country</td>
<td>Disruption in operations for less than one week</td>
<td>&lt;2-3 per cent $200 million-$300 million</td>
<td>Requires intervention from middle management</td>
</tr>
<tr>
<td>2</td>
<td>Moderate</td>
<td>Loss of infrastructure, equipment or other assets</td>
<td>Temporary (i.e., less than 12 months)</td>
<td>One (1) department/office or location: limited impact within department/office or location</td>
<td>Isolated external comments within a country</td>
<td>Moderate disruption to operations</td>
<td>&lt;1-2 per cent $100 million-$200 million</td>
<td>Issues delegated to junior management and staff to resolve</td>
</tr>
<tr>
<td>1</td>
<td>Low</td>
<td>Damage to infrastructure, equipment or other assets</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
</tr>
</tbody>
</table>

#### Likelihood

<table>
<thead>
<tr>
<th>Score</th>
<th>Rating</th>
<th>Certainty</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Expected</td>
<td>&gt;50 per cent</td>
<td>At least yearly and/or multiple occurrences within the year</td>
</tr>
<tr>
<td>4</td>
<td>Highly likely</td>
<td>&lt;50 per cent</td>
<td>Approximately every 1-3 years</td>
</tr>
<tr>
<td>3</td>
<td>Likely</td>
<td>&lt;60 per cent</td>
<td>Approximately every 3-7 years</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>&lt;30 per cent</td>
<td>Approximately every 7-10 years</td>
</tr>
<tr>
<td>1</td>
<td>Rare</td>
<td>&lt;10 per cent</td>
<td>Every 10 years and beyond or rarely</td>
</tr>
</tbody>
</table>

#### Internal Control / Management Effectiveness

<table>
<thead>
<tr>
<th>Score</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Effective</td>
<td>Controls are properly designed and operating as intended. Management activities are effective in managing and mitigating risks</td>
</tr>
<tr>
<td>4</td>
<td>Limited improvement needed</td>
<td>Controls and/or management activities are properly designed and operating somewhat effectively, with some opportunities for improvement identified</td>
</tr>
<tr>
<td>3</td>
<td>Significant improvement needed</td>
<td>Key controls and/or management activities in place, with significant opportunities for improvement identified</td>
</tr>
<tr>
<td>2</td>
<td>Ineffective</td>
<td>Limited controls and/or management activities are in place, high level of risk remains. Controls and/or management activities are designed and are somewhat ineffective in efficiently mitigating risk or driving efficiency</td>
</tr>
<tr>
<td>1</td>
<td>Highly ineffective</td>
<td>Controls and/or management activities are non-existent or have major deficiencies, and do not operate as intended. Controls and/or management activities, as designed are highly ineffective in efficiently mitigating risk or driving efficiency</td>
</tr>
</tbody>
</table>
IV.3 Event Identification and Risk Assessment

Starting with the UN Secretariat risk catalogue, potential risks at department or office level shall be identified by collecting information from relevant management and staff members within the organizational unit that is conducting the risk assessment. The time horizon for the risk identification and assessment should typically be annual. A variety of techniques could be used for data collection, ranging from risk questionnaires and surveys, to individual interviews and workshops, or a combination of those.

IV.3.1 Risk questionnaires and surveys

Whilst risk questionnaires and surveys could be useful to gather information from a wide number of participants in a relatively limited time, their contribution to an effective assessment process is deemed somewhat limited, as they may be perceived as a bureaucratic exercise failing to stimulate proper thinking and discussion on relevant risk areas. In addition, due to lower response rate of surveys, they may not serve as an authoritative data source and shall be complemented by in-person interviews.

IV.3.2 Risk interviews

In light of the limitations surrounding surveys and questionnaires, one-on-one interviews with members of the senior management team appear to be a much more effective and powerful tool. They stimulate important conversations about risks, contributing to the progressive creation and strengthening of a risk aware culture at all levels.

The number of interviews depends on the size and governance structure of the office or department. They should include all the members of the senior management team (D level and above) and a sensible representation of field offices or areas and sections with specific focus or exposure to unique risks. As a general guidance, the UN experience shows that for medium to large entities a number of interviews between 20 and 30 should be able to provide a comprehensive and balanced range of responses.

Linking risks to strategic objectives, they are an excellent vehicle to disseminate information related to risks and a unique source of meaningful discussions. They give the opportunity of confidentially expressing concerns to senior officers who not always might be comfortable in sharing sensitive information in a group setting. Senior officials could of course also choose to hold small workshops instead, inviting to attend a small group of their closest advisors, should they prefer so. Workshops are an excellent opportunity for sharing risk information, thanks to the enriched discussions they generate. One-on-one interviews usually can be effectively completed in about 45 minutes to an hour; small workshops could take slightly longer, in order to give all the participants, the opportunity to effectively contribute to the conversation. It would be ideal if the ERM team could be represented by two colleagues, if possible, one leading the conversation, the other taking detailed notes.

The interviews, which should be of course of confidential nature, are facilitated by the ERM function or the local entity’s Risk Management focal point(s) and require quite a high level of tact and interviewing skills. Starting with the consideration of the relevant objectives for the entity for the period under consideration, and the potential risks to those objectives identified during the initial desk review, as well as taking into consideration the Secretariat risk catalogue, managers are invited to share their views on the most critical risk areas which in their opinion might impact the
ability of the entity to achieve its mandates. Providing a visual representation of the preliminary risks (similar to the Risk Dashboard presented in Figure 4) might help in guiding the discussion.

Managers might start discussing their experience and areas of direct responsibility, and then expand their view to the entire operations of the entity. Personalities might be quite different. Every manager brings to the conversation their individual approach and perspective, and the difference in perspectives represents an important value to the risk assessment process. Some managers might limit to discussing the high level most strategic risks, without providing an opinion on risk ratings and relevant trends, other might have a much more analytical approach and describe in detail risk areas, related drivers and the effectiveness of designed controls and managerial responses. A Sample Questionnaire which could help guide the discussion is provided in Annex 4 of this guide.

It is of course essential that each contribution is properly interpreted by the ERM function and focal points as an important piece to create the mosaic that is the risk register at the entity level. The interview should apply a Socratic approach, eliciting knowledge and understanding of risks through a semi-structured series of questions and answers, acquiring the confidence of the interviewee and at the same time gathering adequate information for the proper analysis of risks and controls.

"I myself know nothing, except just a little, enough to extract an argument from another man who is wise and to receive it fairly.” Socrates

IV.3.3 Risk assessment

Each of the identified risks shall be then evaluated by the ERM team according to the pre-defined risk and internal control rating criteria. As a first step, each risk will be scored in terms of the risk likelihood and impact, based on the information obtained through the interviews, workshops, surveys or process analyses. At this stage, we are considering the "largest credible risk", as the Risk Exposure in the case of simultaneous failure of several controls established to mitigate the risk. From a methodological perspective, for the Secretariat the risk exposure can be determined by taking the square root of impact multiplied by likelihood (resulting therefore in a number between 0 and 5):

\[
\text{Risk exposure} = \sqrt{\text{Impact} \times \text{Likelihood}}
\]

Input to assess the effectiveness of internal controls or managerial processes in place to mitigate the risk should be then evaluated. The proper assessment of internal controls will of course depend on a thorough understanding of their intended purpose – i.e., how they intend to reduce the likelihood or impact of a defined risk, and their operational effectiveness. In practical terms, Residual Risk will be calculated as the difference between risk exposure on one side, and the level of internal control effectiveness on the other, (expressed therefore in a number potentially between -4 and 4):

\[
\text{Residual risk} = \text{Risk exposure} - \text{Level of internal control}
\]
To facilitate the calculation of the residual risk for each risk, the ERM function developed an easy-to-use calculator which is shared on its Community of Practice site\(^2\), as well as, on the ERM page on I-seek.

According to best practice, residual risk is the risk remaining after management has taken action to alter the risk’s likelihood or impact and shall therefore be the starting point for determining the appropriate treatment response. Based on the consideration of the resulting level of residual risk, and most importantly judgement on contributing factors and data gathered during the risk assessment process, risks shall be classified into three tiers.

**Very High risks**, categorised as *Tier 1 (“Red”)* risks, are the most significant risks to which the entity is deemed to be exposed to, and will require an adequate level of attention. They shall be reported to the relevant Head of Office or Department, and the central ERM function, so that they could be consolidated with other risk areas emerging in different areas of the Organization, and accordingly reported to the Management Committee, and through the Secretary-General to the IAAC and the General Assembly.

**High risks** (*Tier 2 – “Orange”*) and **Medium risks** (*Tier 3 – “Yellow”*) will typically require specific remedial or monitoring measures under the responsibility of the specific Risk Owners and local Risk Management Focal Points, under the overall guidance of the relevant heads of entity.

If deemed appropriate by the relevant management, the register might as well include Lower level risks which could materialise quickly and have significant impact in a short span of time, and which should therefore be periodically monitored. Such risks could be as well classified according to their “speed of onset”, or *velocity*. As an example, the risks related to the political volatility of a specific country, and/or the related security situation, could be reflected as **Lower (“Green”)** risks in the Risk Register, as a tool for management to keep the evolving situation under close monitoring, even if the risks as presently assessed were not deemed to be among the most critical.

**IV.3.4 Prioritization**

In order to ensure a strategic and an effective approach, it is important that the assessment focuses on a relatively small number of risk areas with the largest potential to impact the Organization. The vast majority of risks listed in the original risk taxonomy will probably be considered lower level risks, whilst based on the experience of the Organization it is reasonable to expect the risk assessment to consider and analyse in detail approximately the most important 10 to 20 risks. For example, the Secretariat-wide Risk Register has prioritized about 16 very high-risks.

For entities, the prioritization process is crucial, as it should allow creating a short list of 5 to 10 high risk areas (the “top risks”, or “tier 1 risks”) which would require the immediate attention of senior management. Based on the UN experience, even merely listing the risks in order of *residual risk exposure*, from the highest to the lowest, would help to identify a potential gap or threshold above which risks might be considered most critical for the entity. The numerical values above which risks can be considered “Very High”, “High” or “Medium” are shown in the risk calculator, and also depend on the particular risk profile and risk tolerance of the individual entity and continue very much to rely on judgement based on the qualitative elements emerging from the risk assessment process.

\(^2\) https://unitednations.sharepoint.com/sites/DMSPC-BTA_COMMS/SitePages/ERM-Resources.aspx
Prioritization of Fraud and Corruption Risks

As part of a recent specific assessment of fraud and corruption risk areas, the dedicated Advisory Committee considered as “very high” all the risks with a residual risk exposure higher than 1, and “high” the ones between 0 and 1. Risks with a residual risk exposure lower than 0 were considered “medium”.

As mentioned above, it is important to note that numerical values need to reflect the specific risk tolerance of the areas under review, and judgement should be applied considering the specific circumstances.

The entity risk register will not be an exhaustive list of all possible risks, which would be probably extremely long and unmanageable, but a profile of the most significant risks facing the entity, from a senior management strategic perspective. It is also important to note that some flexibility in risk treatment and budget allocation may be applicable to lower risks, as management may decide to implement specific efficiency measures.

The Risk Dashboard, of which an example is reported in Figure 4 below, is an effective tool to visualise the initial results of the assessment, collecting the emerging risks under the main categories of the taxonomy and representing their classification according to the three tiers and the corresponding colour codes (red for very high risks, orange for high risks, and yellow for medium risks).
**Figure 4 – Example of a Risk Dashboard** (for illustration purposes only)

<table>
<thead>
<tr>
<th>STRATEGIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning and Resources Allocation</td>
</tr>
<tr>
<td>Vision, Mandate &amp; Public Perception (1.1.1)</td>
</tr>
<tr>
<td>Strategic Planning, Budgeting (1.2.2)</td>
</tr>
<tr>
<td>Org Culture, HR Strategy &amp; Acct (2.1.7)</td>
</tr>
<tr>
<td>Org, Transf., Mgmt. Reform (1.3.10)</td>
</tr>
<tr>
<td>Principal Organs, and Partners</td>
</tr>
<tr>
<td>Gd, Committees and Member States (2.2.1)</td>
</tr>
<tr>
<td>Partnership and Coordination (2.2.2/3)</td>
</tr>
<tr>
<td>Internal and External Factors</td>
</tr>
<tr>
<td>Political Climate (3.1.1/2)</td>
</tr>
<tr>
<td>Parastats (3.1.4)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GOVERNANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
</tr>
<tr>
<td>Control Environment and Risk Mgmt. (1.1.2)</td>
</tr>
<tr>
<td>Organization Structure &amp; Synchronization (2.1.3)</td>
</tr>
<tr>
<td>Eth, Professional Conduct (2.2.1)</td>
</tr>
<tr>
<td>Sexual Exploitation &amp; Abuse (2.2.3)</td>
</tr>
<tr>
<td>Gd, Committees and Member States (2.2.1)</td>
</tr>
<tr>
<td>Partnership and Coordination (2.2.2/3)</td>
</tr>
<tr>
<td>Internal and External Factors</td>
</tr>
<tr>
<td>Political Climate (3.1.1/2)</td>
</tr>
<tr>
<td>Parastats (3.1.4)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MANAGERIAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
</tr>
<tr>
<td>Mgmt. of Orgn, Transformation (3.1.1)</td>
</tr>
<tr>
<td>Leadership and Management (3.1.7)</td>
</tr>
<tr>
<td>Staff/Management Relations (3.1.3)</td>
</tr>
<tr>
<td>Mission Activities</td>
</tr>
<tr>
<td>Fiduciary and SPM Governance (5.3.1)</td>
</tr>
<tr>
<td>Mission Planning (5.3.4)</td>
</tr>
<tr>
<td>Knowledge &amp; Infm, Management (4.3.1/2)</td>
</tr>
<tr>
<td>Information Resources</td>
</tr>
<tr>
<td>ICT Strategy and Infrastructure (4.4.1/5)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPERATIONAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support Services</td>
</tr>
<tr>
<td>Procurement &amp; supplier Mgmt. (4.1.1)</td>
</tr>
<tr>
<td>Facilities &amp; Real Estate Mgmt. (4.1.5)</td>
</tr>
<tr>
<td>Risk and Compliance (4.4.2)</td>
</tr>
<tr>
<td>Information Security (4.1.6)</td>
</tr>
<tr>
<td>Security (4.2.11)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FINANCIAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Funding and Investments</td>
</tr>
<tr>
<td>Financial Contributions (5.1.1)</td>
</tr>
<tr>
<td>AB Mgmt. and Implementations (5.1.4/5)</td>
</tr>
<tr>
<td>SME System Control Environment (5.1.3)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FRAUD and CORRUPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Environment</td>
</tr>
<tr>
<td>ICT Governance and Cyber Security (7.1.2)</td>
</tr>
<tr>
<td>Programme Delivery</td>
</tr>
<tr>
<td>Political Influence on Proj, Imp., &amp; Reporting (7.2.1)</td>
</tr>
<tr>
<td>Contingent-Owned Equipment (7.2.3)</td>
</tr>
<tr>
<td>Theft, Fraud, Embezzlement, Inventory (7.2.4)</td>
</tr>
<tr>
<td>Human Resources and Central Services</td>
</tr>
<tr>
<td>HR Fraud and Corruption (7.3)</td>
</tr>
<tr>
<td>Procurement Fraud (7.4.1)</td>
</tr>
<tr>
<td>False Statements and False Power (7.4.3)</td>
</tr>
</tbody>
</table>

Legend: Red - Critical and Very High; Orange - High; Yellow - Medium; Green - Low

Note: The above Risk Dashboard is a representation of a potential outcome from a Risk Assessment and is provided for illustrative purposes only.

If needed to visualise the distribution of risk areas, the **Residual Risk Heat Map**, a four-quadrant chart as depicted in Figure 5 below, could also provide a graphic representation of the results of the risk assessment, and in particular of the residual risks as a function of risk exposure and level of internal control effectiveness, assisting management in the determination of appropriate risk treatment strategies and risk mitigation measures.
IV.3.4 Alignment of risks with Mandates, Objectives and Strategic Plans

ERM is driven by organizational strategies and objectives, and the processes and initiatives designed to achieve them. The ability to appropriately link risks to strategies and objectives and the underlying processes and activities is critical to the identification and implementation of effective risk mitigation measures. The template represented in Figure 6 below could support management in this process.

Note: The above Residual Risk Map is a representation of a potential outcome from a Risk Assessment, and is provided for illustrative purposes only.
The risk assessment, through the alignment of risks with objectives and plans, effectively facilitates the relationship between the risk management process and budgeting. The output from the risk assessment shall be a key driver and input in supporting decision making around budget priorities and requirements.

Figure 6 – Example of an alignment of risks to objectives
(for illustrative purposes only)

<table>
<thead>
<tr>
<th>Risk Number</th>
<th>Risk Definition</th>
<th>Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.2</td>
<td>Strategic Planning</td>
<td>VH VH VH</td>
</tr>
<tr>
<td>1.1.4</td>
<td>Budget Allocation</td>
<td>H H H</td>
</tr>
<tr>
<td>1.1.7</td>
<td>Organizational Synchronization</td>
<td>M M M</td>
</tr>
<tr>
<td>2.1.3</td>
<td>Control Environment</td>
<td>H H H</td>
</tr>
<tr>
<td>2.1.5</td>
<td>Organizational Structure</td>
<td>M M M</td>
</tr>
<tr>
<td>2.1.6</td>
<td>Performance Measurement</td>
<td>H H H H</td>
</tr>
<tr>
<td>2.1.9</td>
<td>Transparency</td>
<td>M M M</td>
</tr>
<tr>
<td>2.1.11</td>
<td>Accountability</td>
<td>VH VH VH</td>
</tr>
<tr>
<td>2.1.12</td>
<td>Empowerment</td>
<td>H H H H</td>
</tr>
<tr>
<td>2.2.1</td>
<td>Ethics</td>
<td>M M M</td>
</tr>
<tr>
<td>2.2.2</td>
<td>Fraud &amp; Illegal Acts</td>
<td>H H H H</td>
</tr>
<tr>
<td>2.2.3</td>
<td>Conflicts of Interest</td>
<td>M M M</td>
</tr>
<tr>
<td>2.4.1</td>
<td>Public Perception, Support, Reput</td>
<td>H H H H</td>
</tr>
<tr>
<td>3.4.3.1</td>
<td>Procurement: Requisition</td>
<td>VH VH VH</td>
</tr>
<tr>
<td>3.4.3.2</td>
<td>Procurement: Strategy</td>
<td>VH VH VH</td>
</tr>
<tr>
<td>3.4.3.3</td>
<td>Procurement: Bidding &amp; Bid Evaluation</td>
<td>VH VH VH</td>
</tr>
<tr>
<td>3.4.4</td>
<td>Vendor Management</td>
<td>VH VH VH</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Resource Allocation &amp; Availability</td>
<td>VH VH</td>
</tr>
<tr>
<td>3.5.2</td>
<td>Recruiting, Hiring &amp; Retention</td>
<td>H H H</td>
</tr>
<tr>
<td>3.5.9</td>
<td>Training</td>
<td>M M M</td>
</tr>
<tr>
<td>3.7.1</td>
<td>IT Strategy &amp; Implementation</td>
<td>VH VH VH</td>
</tr>
<tr>
<td>3.7.5</td>
<td>IT Infrastructure &amp; Systems</td>
<td>VH VH VH</td>
</tr>
<tr>
<td>4.1.1.1</td>
<td>Contract: Administration &amp; Issuance</td>
<td>M M</td>
</tr>
<tr>
<td>4.1.1.2</td>
<td>Contract: Management</td>
<td>VH VH</td>
</tr>
</tbody>
</table>

Note: The above alignment of risks to objectives is a representation of a potential outcome from a Risk Assessment and is provided for illustrative purposes only.

IV.3.5 Validation workshop

The results of the assessment shall be ultimately validated in a dedicated senior management workshop so that management could share a common understanding of the identified risks, their criticality, and the risk response strategies that should be considered. Senior management workshops at entity level, chaired by the head of entity with the participation of the senior management team, are an essential step in the ERM implementation process, as they contribute to sustain and embed a risk-aware culture at the highest level.

As mentioned before, workshops are an excellent opportunity for sharing risk information, generating enriched conversations on future uncertainties and relevant mitigation strategies. They are conducted under the overall leadership of the head of entity with the facilitation being provided by the ERM function and/or the local Risk Management focal point(s). They cover a central role in
the ERM implementation process, directly engaging senior managers in discussions on mandates and objectives, and the risks or uncertainties in effectively achieving them within commonly agreed tolerances. The results of the discussion, aiming to reach consensus on the critical risks, response strategies, and risk ownership, should be fully reflected in the final Risk Register. It is important to note that the final approved Risk Register might differ from the initial draft, as it aims to represent the collegial views of the head of entity and the senior management team.

The Risk Register will include the Risk Universe for the entity (the risk category, sub-category, and risk definition), and further information regarding rating results, risk drivers, and potential risk response strategies. A Risk Register template is attached as Annex 5. The Register should be constantly maintained and updated, reflecting any relevant changes in the risk environment. A formal comprehensive risk assessment shall be undertaken annually.

IV.4 Risk Response and Internal Control Activities

Based on the high-level response strategies agreed by senior management and summarized in the Risk Register, Risk Owners shall design a detailed Risk Treatment and Response Plan.

Determination of Risk Responses

The quadrant of the Residual Risk Heat Map in which each risk is plotted could facilitate the determination of the proposed risk treatment, broadly falling into four categories:

(i) **Risk Reduction** – Risks characterised by a high-risk exposure and ineffective internal controls will fall in the “risk reduction” quadrant. A reduction in risk exposure could be achieved through different strategies, such as:

   (a) the adoption of prevention plans aimed at reducing the likelihood of a risk occurring by treating the risk contributing factors;

   (b) the deployment of response strategies, formulating an appropriate risk treatment, should the risk materialise; or

   (c) the transfer of risk exposures to external parties through mechanisms as insurance or outsourcing.

(ii) **Risk Acceptance or Optimisation** – Risks falling into this category have a low risk exposure and a level of internal control effectiveness deemed high. Risk may be therefore accepted, as considered either inherent in the environment, or an integral part of the activities necessary to achieve defined objectives.

   Other risks may be deemed to be overly controlled, as the level of adopted control measures may reduce the ability of the Organization to effectively achieve stated objectives, or the cost of the internal control activities may be considered to exceed any derived benefits.

(iii) **Risk Monitoring** – Risks with a relatively low risk exposure and low internal control effectiveness will be included in this category. As even if these risks were to materialise, the impact on achievement of objectives would be modest, no improvement in internal control effectiveness would be normally required. The Risk Owner, with support of the local Risk Management Focal Point(s), shall
perform regular risk monitoring activities, so that any potential increase of the risk exposure could be timely identified.

(iv) **Internal Control Monitoring** – With regard to the significant risks that are deemed to be appropriately managed, an assessment process effected by the Risk Owner and the local Risk Focal Point, and oversight activities carried out by other monitoring functions, including Internal Audit, shall provide assurance on the ongoing effectiveness of designed internal controls.

**Internal Controls**

As mentioned previously, according to the best international standards, an effective system of internal control is encompassed within and an integral part of enterprise risk management. Enterprise risk management is deemed to be broader than internal control, expanding and elaborating on internal control to form a more robust conceptualisation and tool for management.

Control activities are an essential part of the process by which the Organization seeks to achieve its objectives. They consist of the policies and procedures that help ensure that management’s risk responses are carried out properly and in a timely manner, and include a range of activities, as diverse as approvals, authorisations, verifications, reconciliations, reviews of operational performance, physical controls, and segregation of duties. Preventive controls are in particular designed to limit the possibility of a risk maturing and an undesirable outcome being realised. Detective controls are conversely designed to identify whether undesirable outcomes have occurred “after the event”.

With regard to the identified risks, comprehensive **Risk Treatment and Response Plans** shall outline the main controls that management has already established, and the additional control and treatment strategies management plans to introduce to further mitigate risks, as may be appropriate, defining detailed action plans, timelines, and identifying risk treatment owners, as illustrated by Figure 7 below.

---

**Case study**

**Implementation of a detailed risk treatment plan for the “Extra-budgetary Funding and Management” risk in the context of the Secretariat-wide framework**

**The Secretariat-wide Risk Register**

The results of the enterprise-wide risk assessment are captured in the UN Secretariat’s Risk Register. Risks are classified into tiers based on the qualitative evaluation of exposures and control effectiveness as well as contributing factors gathered during the risk assessment process. The Management Committee validates the Risk Register to come to a common, shared understanding of risks and their criticality, identifying the risks on which immediate action is needed and the managers (Corporate Risk Owners) responsible for the definition of Risk Treatment and Response Plans. The Register is ultimately formally approved by the Secretary-General.

In their role, **Corporate Risk Owners** are supported by **Risk Treatment Working Groups**, comprised of members of different entities representing the different functional areas of the
Under the guidance of the respective Corporate Risk Owners, Working Groups define detailed Risk Treatment Plans for each of the critical risks, approved by the Management Committee, as ERM Committee for the Organization, and monitor the work of the responsible risk treatment teams, the effectiveness of the agreed actions in mitigating the risks, and the evolving risk profile of the Organization, with periodic reporting to the Committee.

Extra-budgetary Funding and Management

The Management Committee and the Secretary-General deemed Extra-budgetary Funding and Management as one of the critical risks for the Organization and nominated the Controller as the risk owner at the corporate level. The risk is defined as: "The inability to obtain extra-budgetary funding may impact the ability of certain departments to achieve their objectives. Reliance upon extra-budgetary funding may jeopardize or appear to impact the independence of the UN as projects that obtain earmarked funding may be given higher priority. Inability to identify, establish and maintain the optimal structure and controls for trust funds resulting in loss or misuse of assets."

Key drivers include:

- Donors might change priorities or move resources to other actors. Inherent instability of the operations and impact on the ability to plan strategically.
- Reliance on a few donors for a large portion of extra-budgetary funding and lack of predictable funding may be perceived as potentially influencing the Organization to focus on donor countries’ priorities and impacting its credibility.
- Loss in extra-budgetary funding will impact the programme support accounts and may also significantly affect the Organization’s regular programme of work.
- Delay in anticipated cash against pledges and projected income may impact operations of the Organization negatively.
- Trust fund managers may have limited mechanisms to ensure stewardship of funds by implementing agencies and to enforce proper reporting on the use and impact of funds.
- Potential weaknesses in the establishment and maintenance of adequate controls on the use and impact of funds, and to mitigate fiduciary or corruption risks, could expose the Organization to significant reputational issues.
- Different reporting systems established by donors and inadequate accountability frameworks may impact the ability to measure the outcomes of XB funded activities.

Potential Risk Response strategies involve:

- Development of a comprehensive multi-year resource mobilization strategy. Advocacy for an increase in the number of donor countries.
- Monitoring the effectiveness of systems designed to manage project-related funds; improving the timeliness and comprehensiveness of reporting.
- Holding implementing entities accountable for appropriate use and timely and accurate reporting of the usage of funds.
- Administering and managing extra-budgetary resources with the same rigour as regular budgets.
The Risk Treatment Plan

Under the guidance of the Controller, the dedicated working group defined and implemented a detailed risk treatment plan structured around three main areas:

1. **Standardization of donor agreements**
   - (a) Institute Secretariat-wide agreements with key donors
   - (b) Issue a clear guidance on restrictive conditions (e.g.: immunities and privileges of the United Nations, single audit principle, procurement, recruitment)
   - (c) Establish a set of minimum required clauses for each agreement, such as standardization of donor reports, annual reporting, evaluations, and contribution payment terms

2. **Management of implementing partners**
   - (a) Formulate a corporate guidance on standard procedures for selecting implementing partners (IPs), which will clarify the difference between the IP selection process from the procurement process, and between Implementing Partnerships and Grants
   - (b) Establish a robust contract management to follow-through funds transferred to IPs
   - (c) Make the evaluation of IPs available Secretariat-wide and issue a guidance on how to deal with IPs that do not deliver

3. **Update of internal controls mechanisms that govern the administration of trust funds**

**The implementation**

As part of the work of the risk treatment group, the Organization issued guidance on restrictive conditions (e.g.: immunities and privileges of the United Nations, single audit principle, procurement, recruitment), and established a set of minimum required clauses for each agreement, such as standardization of donor reports, annual reporting, evaluations, and contribution payment terms. Policies for establishing and managing trust funds (ST/SGB/188) and relevant administrative instructions (ST/AI/284, ST/AI/285) have been updated and circulated to the Secretariat’s Finance community.

Corporate guidance on standard procedures for selecting implementing partners (IPs), clarifying the difference between the IP selection process and the procurement process, and between Implementing Partnerships and Grants, is in process of formulation in consultation with programme managers and OLA. The Working Group also analysed proposals to put in place a corporate fraud sanction procedure for implementing partners. The policy is currently being refined, taking into account lessons-learned from other UN agencies.

The implementation of the Working Group’s action plan serves as the basis for the Organization’s medium-term strategy for further securing and expanding extra-budgetary funding.
IV.5 Information and Communication

Relevant risk and internal control information shall be provided at the appropriate levels within the Organization, to adequately support decision making towards the achievement of established mandates and objectives.

**Entity level risk assessment results**

The results of the different risk assessments shall be collected by the Enterprise Risk Management function and compared within and across unit locations. All risk definitions and criteria shall ultimately be aligned to those established at the Organization level. Risk results may be compiled and aggregated, as an important input to the Secretariat-wide Enterprise Risk Assessment and Risk Register. The results of the entity level assessment shall facilitate the Organization’s ability (at the Secretary-General, Management Committee and General Assembly level) to understand and effectively integrate risk assessment outputs into strategic decision-making activities.

**Results based management**

The results of the enterprise risk management process shall be leveraged to support decision-making in strategic planning, budgeting, and allocation of resources. In this perspective, the risk reports described in the following section of this document shall be provided to senior management and governing bodies as part of the reporting and submission phases of the programme planning and budget preparation.

The risk profile of the Organization and the effectiveness of the designed controls shall be fully considered in setting the funding and resource allocation requests as part of the programme planning and budgeting process. An effective enterprise risk management and internal control process will therefore become instrumental to the promotion of a risk driven culture through a more informed risk based decision-making capability, as the significance of risks and the effectiveness of dedicated internal controls will be explicitly considered when evaluating programmes and relevant budget allocations, effectively setting in this process the risk tolerance of the Organization with regard to specific risks and programmes.

**Risk reporting and frequency**

The risks to be reported on, the level of required details, and the frequency of reporting shall depend on the audience. Sufficient information about the risks and associated risk management and internal control activities shall be provided, so that recipients are able to fulfil their risk management responsibilities. Risk and internal control information concerning risks deemed to be of the greatest significance on an Organization-wide basis shall be summarised and provided to the Secretary-General, and through the Secretary-General, the General Assembly and the Advisory Committee on Administrative and Budgetary Questions (ACABQ) and IAAC, whilst detailed information covering their area of responsibility shall be distributed to the managers responsible for the management of specific risks.

The frequency of risk reporting also depends upon the report recipients. At Secretariat-wide level, *annual reporting* is established to the General Assembly, through the ACABQ and IAAC, whilst *quarterly reporting* is defined for the Management Committee, and through the Management Committee...
Committee, the Secretary-General. Regarding local level risk registers and risk treatment and response plans, Heads of entity and local senior management teams shall receive quarterly reports.

Relevant risk and internal control information shall be provided in line with the reporting and submission phases of the programme planning and budget preparation, where applicable.

In terms of reporting modalities to the ERM Section, annual reporting requirements by Heads of Entities are established, in recognition of their special responsibility for defining and maintaining accountability mechanisms in line with the new management paradigm of delegation of authority. To discharge this responsibility, it is imperative that Risk Management Focal Points keep senior management fully informed on status of risk management in their respective entities, including identified risks, recommendations to mitigate them and practical actions taken in this regard.

To facilitate this process, BTAD/ ERM, has developed the attached template (Annex 6) for reporting the status of risk management by the entities. The report should be completed by the Risk Management Focal Point within 30 days following the end of the year and submitted to the USG/ DMSPC. In addition to this, Peacekeeping Operations and Special Political Missions Operations should also submit the report to the USGs of DPO and DPPA.

According to best practices, the annual risk reports that shall be prepared in support of risk management activities take into consideration the following elements.

(i) **UN Secretariat-wide Risk Register** – The Risk Register summarises the most significant risks at Organization level. It includes:

(a) Executive summary

(b) *Risk Dashboard* - a graphical representation of the significant risks identified as a result of the risk assessment process, and for each risk:

(c) Risk definition

(d) Risk scoring in terms of impact, likelihood and control / management effectiveness

(e) Residual risk classification

(f) Factors that contribute to the risk (key drivers)

(g) Relevant controls designed by management

(h) An overview of the risk response strategy

(i) Risk ownership

(j) Strategic Objectives of the Organization

(k) Secretariat Risk Universe

(l) Scoring Criteria for the measurement of Impact, Likelihood and level of Control Effectiveness

To facilitate the prioritization and identification of response strategies, risks might as well be charted on a Residual Risk Heat Map.

The Risk Register is formally revised by the Enterprise Risk Management function following the *biennial Secretariat-wide risk assessment* process and distributed to the Management Committee and the Secretary-General. Through the Secretary-
General, a summary is distributed to the General Assembly through the ACABQ, and the IAAC.

The Register is constantly monitored and updated to reflect the changing risk profile of the Organization, as it might be needed, following quarterly reviews and discussion at Management Committee level.

(ii) **Risk Register at the Entity level** – Following the same template of the Secretariat-wide Risk Register, the local register reflects the results of the organizational unit’s risk assessment. The Risk Register is distributed to the head of department or office, the senior management team - as local ERM Committee, and the ERM function, following its formal periodic (annual) revision. Entities shall continue to provide annual reports to the central ERM function in DMSPC. The template for reporting by entities of the results of the annual risk assessment is provided in the ERM’s Community of Practice Site³ and included in Annex 6.

Notwithstanding the annual reporting requirement, the risk register should be treated as a live document and reviewed regularly to monitor any changes in the risk profile and identify emerging risks. Quarterly presentations by the risk focal points to the local level ERM committee are a powerful tool to ensure the continued attention of the whole senior management team on the most critical risk areas the entity is facing, a prompt identification of significant changes in its overall risk profile, and the consideration of emerging risks.

(iii) **UN Secretariat-wide Risk Treatment and Response Plan** – Regarding the most significant risk areas identified, a comprehensive Risk Treatment and Response Plan is prepared by the Risk Owners at corporate-level, considering the advice of dedicated working groups comprised of “subject matter experts”, and approved by the Management Committee, as Enterprise Risk Management Committee for the Organization. The Risk Treatment and Response Plan summarises the managerial response designed to appropriately mitigate the risks. It includes:

(a) Executive summary, and for each risk:

(b) Risk definition, risk scoring in terms of impact, likelihood and control / management effectiveness, residual risk classification and risk ownership

(c) Risk treatment specific actions

(d) Due dates

(e) Responsible teams

Corporate Risk Owners present quarterly updates to the Management Committee, on the progress of the implementation of the risk treatment plan and on the evolving nature of the risks under their area of responsibility. A Risk Treatment and Response Plans Progress Scorecard is prepared to highlight progress in the implementation of the Risk Treatment and Response Plans, as well as areas on which attention of the Management Committee, as ERM Committee for the Organization, might be required. The Scorecard is presented in two parts:

a) An Executive Summary, which provides a colour code dashboard visually representing the status of implementation for each of the major groups of actions in the Risk Treatment and Response Plans (a sample is shown in figure 8a)

³ https://unitednations.sharepoint.com/sites/DMSPC-BTA_COMMS/SitePages/ERM-Resources.aspx
b) A Progress Scorecard, which provides a comprehensive assessment on the status of implementation for each of the risk treatment actions, as well as due date and scoring (a sample is shown in figure 8b)

Outlines of the Risk Treatment and Response Plan are presented to the General Assembly through the ACABQ, and the IAAC.

### Figure 7 – Example of a Risk Treatment and Response Plan

<table>
<thead>
<tr>
<th>5. Extra-budgetary Funding and Management (S.1.10/50.14)</th>
<th>Risk category</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Internal Control Effectiveness</th>
<th>Residual Risk</th>
<th>Corporate Risk Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td></td>
<td>5 – Critical</td>
<td>4 – Highly likely</td>
<td>3 – Significant improvement needed</td>
<td>Critical</td>
<td>Controller</td>
</tr>
</tbody>
</table>

**Risk Definition**

The inability to obtain extra-budgetary funding may impact the ability of certain departments to achieve their objectives. Reliance upon extra-budgetary funding may jeopardize or appear to impact the independence of the UN as projects that obtain earmarked funding may be given higher priority. Inability to identify, establish and maintain the optimal structure and controls for trust funds resulting in loss or misuse of assets.

<table>
<thead>
<tr>
<th>Treatment plan</th>
<th>Working Group Members: OPPBA, ECA, Habitat, OCHA, OHRQ, OUSG-OIM, UNOCC, DESA, Ethics Office</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Risk Treatment Action</th>
<th>Due Date</th>
<th>Responsible Team</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Standardization of donor agreements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Institute Secretariat-wide agreements with key donors</td>
<td>Dec 2015</td>
<td>OPPBA</td>
</tr>
<tr>
<td>b. Issue clear guidance on restrictive conditions (e.g. immunities and privileges of the United Nations, single audit principle, procurement, recruitment)</td>
<td>Dec 2015</td>
<td>OPPBA</td>
</tr>
<tr>
<td>c. Establish a set of minimum required clauses for each agreement, such as standardization of donor reports, annual reporting, evaluations, and contribution payment terms</td>
<td>Dec 2015</td>
<td>OPPBA</td>
</tr>
<tr>
<td>2. Management of implementing partners</td>
<td></td>
<td></td>
</tr>
<tr>
<td>a. Formulate a corporate guidance on standard procedures for selecting implementing partners (IPs), which will clarify the difference between the IP selection process from the procurement process, and between Implementing Partnerships and Grants</td>
<td>Nov 2015</td>
<td>OPPBA</td>
</tr>
<tr>
<td>b. Establish a robust contract management to follow-through funds transferred to IPs</td>
<td>Dec 2015</td>
<td>OPPBA</td>
</tr>
<tr>
<td>c. Make the evaluation of IPs available Secretariat-wide and issue a guidance on how to deal with IPs that do not deliver</td>
<td>Jun 2016</td>
<td>OPPBA</td>
</tr>
<tr>
<td>3. Update of internal controls mechanisms that govern the administration of trust funds</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The above Risk Treatment and Response Plan is a representation of a potential outcome from a Risk Assessment and is provided for illustrative purposes only.
Figure 8a – Example of a Risk Treatment and Response Plan Progress Scorecard

Executive Summary

1. Strategic Planning, Budgeting and Budget Allocation
   1. Strategic planning
   2. Assess funding and resource needs
   3. Identify strategic priorities
   4. Improve financial management
   5. Strengthen budget processes

2. Organisational Structure and Synodisation
   1. Integrate organisations with others
   2. Deepen governance
   3. Strengthen the effectiveness of central management
   4. Ensure defined organisational functions and reporting lines

3. Healthcare Management
   1. Implement safety first and risk
   2. Undertake compliance assessment of healthcare
   3. Improve evidence-based guidance and,(UK Health Care
   4. Measure and report clinical adverse event reports
   5. Conduct analysis to identify trends
   6. Establish a mechanism for data sharing
   7. Develop an electronic database
   8. Ensure access to mental health & primary care services

4. Occupational Safety and Health
   1. Confirm Management System (OSHA) inspection
   2. Complete OSHA inspection
   3. Undertake OSHA review of mental health
   4. Establish OSHA safety protocols for local committees
   5. Establish OSHA Health and Safety
   6. Establish OSHA safety protocols for local committees
   7. Identify Processional hazards

5. Pandemics
   1. “World Pandemic Draft Plan”
   2. Final Health Pandemic Plan
   3. Establish emergency mechanism for political coordination
   4. Provide science to UN Health and Public
   5. Determine medical emergency measurements
   6. Support operations in field and health centers
   7. Ensure additional support to healthcare settings
   8. Establish health communication mechanisms

6. ICT Strategy, Infrastructure, Statistics and Processing
   1. Align ICT strategies and processes
   2. Define ICT infrastructure
   3. Ensure collaboration between the teams and ICT
   4. Strengthen internal controls
   5. Ensure organisational and strategic

7. ICT Governance and Cyber Security
   1. Strengthen internal controls
   2. Design an ICT governance structure
   3. Strengthen ICT monitoring
   4. Progress Action Plan
   5. Improve information and cyber security

Legend:
- Completed
- On Track
- Partially Completed / Delays
- Not Started / Not Met

To show the status of implementation for risk treatment actions, colour codes are used as follows:

- ‘Blue’ represents risk treatment actions/tasks that are fully completed.
- ‘Green’ represents risk treatment actions/tasks that are on track.
- ‘Yellow’ represents risk treatment actions/tasks that are partially completed or will potentially miss their target implementation date.
- ‘Red’ represents risk treatment actions/tasks that have not started yet or are going to miss their target implementation date.

Figure 8b – Example of a Progress Scorecard for a specific risk including its relevant treatment actions

<table>
<thead>
<tr>
<th>Treatment Action</th>
<th>Progress</th>
<th>CRO: EOBG</th>
<th>Red Chair: TTO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. – Integrate Secretariat-wide results-based and risk management approaches and support the allocation of budgetary resources.</td>
<td>- DMRSP/OPPM introduced a policy guidance for programme managers on how to assess risk of reduced assessed and voluntary contributions on their mandate delivery.</td>
<td>Ongoing</td>
<td></td>
</tr>
<tr>
<td>2. – Strengthen accountability for use of resources and delivery of results.</td>
<td>- DMRSP/OPPM prepared comprehensive management reports and dashboards to detect and proactively address weaknesses in delivery as well as compliance issues.</td>
<td>Ongoing</td>
<td></td>
</tr>
<tr>
<td>3. – Improve management information for budgetary planning and decision-making.</td>
<td>- DMRSP undertook enhancement of UVE 2018 to improve programme performance and information on resources.</td>
<td>Ongoing</td>
<td></td>
</tr>
<tr>
<td>4. – Strengthen budget preparation, review and implementation processes.</td>
<td>- DMRSP/OPPM improved the format/presentation of programmatically, financial and performance information to Member States.</td>
<td>Ongoing</td>
<td></td>
</tr>
</tbody>
</table>

27
(iv) **Risk Treatment and Response Plan at the Entity level** – Following the same template of the Secretariat-wide Risk Treatment and Response Plan, the local plan reflects the managerial response to the risks identified at the organizational unit’s level. The plans are designed by Risk Owners at the entity-level and approved by the local ERM Committee, which shall then receive quarterly updates on progress.

Risk Owners could be supported in their responsibilities of defining and implementing risk treatment actions by working groups comprised of thematic experts from across the entity, as deemed appropriate by the local ERM Committee. The Enterprise Risk Management function shall provide overall coordination and guidance to the process. The template of the Risk Treatment and Response Plan is provided in the ERM’s Community of Practice Site⁴.

**Note**

**Escalation of risks beyond the scope of the responsibilities of the entity**

As mentioned before, “Very High” risks, categorised as *Tier 1* risks at the entity level, shall be reported to the central ERM function. As a result of the risk assessment process, entities might as well identify risks for which an effective response should be taken at organization-wide level, and whose management therefore goes beyond the responsibilities of the organizational unit. Such risks should as well be reported to the central ERM function, so that they could be consolidated with other comparable risks emerging in different areas of the Organization, and accordingly reported to the Management Committee, and through the Secretary-General to the IAAC and the General Assembly. Their consideration at the appropriate level allows the Organization to define and implement an adequate corporate level response.

An example could be provided by *Human Resources Strategy and Management* matters. As a result of the entity level risk assessment, departments and offices reported issues as follows:

- The recruitment of qualified and motivated staff and the development of a results and performance-oriented culture are not effectively supported by the existing policies and procedures, hindering the formulation of HR strategies and career planning mechanisms.
- The performance rating system is unable to adequately reflect staff performance.
- Limited consequences are in place to sanction staff and managers for not meeting goals.
- Absence of incentives to reward performance and of opportunities for promotion.
- The Organization’s approach to organizational learning and development is not clearly linked to planning, knowledge management, guidance, training, monitoring and evaluation.

It is evident that an effective response to those issues can be taken only if the risk is managed under the leadership of the USG-DOS and ASG-OHR and the overall guidance of the Management Committee. Regarding those matters, a dedicated working group comprised of thematic experts may be established to progressively review and implement a risk response, including:

⁴ [https://unitednations.sharepoint.com/sites/DMSPC-BTA_COMMS/SitePages/ERM-Resources.aspx](https://unitednations.sharepoint.com/sites/DMSPC-BTA_COMMS/SitePages/ERM-Resources.aspx)
- The development of a HR strategy incorporating a stronger talent management element to support a performance-oriented culture.
- Enhancements of workforce planning through the revision of relevant policies and procedures.
- The re-evaluation of the effectiveness of the performance management rating system.
- Rewarding high-performing individuals and teams, considering actions with no financial impact, as well as mechanisms for promotion.
- Holding managers and staff accountable for non-performance against pre-defined criteria.

IV.6 Monitoring and Assurance

As the environment in which the UN Secretariat operates is constantly changing, the continuous monitoring and review of risk information is crucial to ensure its continued adequacy for effective decision-making. Risk Owners and Risk Treatment Owners shall accordingly ensure relevant information remains current or is appropriately re-evaluated in case of specific events or circumstances that could affect the risk profile of their areas of responsibility.

As the risk assessment process relies on management’s perception of internal control effectiveness, adequate assurance activities shall as well validate the evaluation, providing assurance regarding the effectiveness of designed controls and the appropriateness of defined risk treatments. The local Risk Management Focal Points and the ERM function shall assist management with ongoing monitoring and reporting.

The Office of Internal Oversight Services (“OIOS”) will be responsible for the independent evaluation of the effectiveness of the internal control environment, in accordance with its mandate, including the periodic assessment and evaluation of the implementation of an effective enterprise risk management and internal control framework.

The Board of Auditors, as part of the assurance activities regarding the financial statements of the Organization described by its charter and mandate, will continue to assess the effectiveness of the system of internal control adopted by the Organization.

Enterprise risk management and internal control technology and tools

In support of the described enterprise risk management and internal control framework programme, the Secretariat requires the capability to automate many of the activities, tools, and reports critical to the programme’s successful implementation. The automation of the framework shall provide a consistent and structured method for identifying, assessing, monitoring, and communicating risks and internal controls associated with the various activities, processes and functions across the Organization.

The IT solution for ERM shall be designed to incorporate the various and diverse elements of the framework, including a linked database repository of risks and risk information (the risk register), and the capability to support and measure risk at different levels within the Organization. The system shall be accessible on a global scale with established access and user rights as defined for each user group and shall have advanced reporting and data management capabilities. DMSPC
plans to roll out an information technology tool that will automate the implementation of ERM across the Secretariat.

V. Risk Governance, Roles and Responsibilities

The Guide has so far presented the definitions of both risk and ERM and introduced the ERM framework that outlines the major steps of the ERM process cycle. This last section will describe the risk governance mechanisms, and the roles and responsibilities of the different functions involved.

**Figure 9 – Risk governance structure**

![Risk governance structure diagram]

**General Assembly**

The General Assembly, with the advice of the ACABQ and IAAC, is responsible for determining the risk tolerance of the Organization\(^5\). The General Assembly covers also a key role in ensuring that senior management adopts and maintains an effective enterprise risk management and internal control framework.

---

Secretary-General

Ultimate responsibility for effective risk and internal control management within the Secretariat resides with the Secretary-General. With the assistance of the Management Committee, the Secretary-General periodically reviews the significant risks facing the Organization, as well as the proposed strategies designed to effectively mitigate the identified risks at a consolidated corporate level, and reports accordingly to the General Assembly and the IAAC.

Management Committee

The Management Committee, in its role as the ERM Committee for the Organization, provides guidance and direction regarding the implementation of ERM in the Secretariat, and monitors the effectiveness of the overall ERM and internal control framework. In this capacity, the Committee validates the Secretariat-wide Risk Register and come to a common understanding of risks and their criticality and identifies the risks on which immediate action is needed. It further approves the risk governance structure and identifies the managers (Corporate Risk Owners) responsible for the definition of Risk Treatment and Response Plans.

The Committee quarterly reviews the risk profile of the Secretariat and the adequacy of risk response strategies and has an active role in the promotion of the best practices in risk and internal control management in the Organization.

Under-Secretary-General for Management Strategy, Policy and Compliance

The USG/DMSPC serves as the high-level official responsible for leading the ERM implementation in the Secretariat. The USG/DMSPC also chairs the Management Committee ERM Task Force, which is composed of the "Corporate Risk Owners" as identified in the Risk Register and the USG for OIOS in an advisory capacity.

Management Committee ERM Task Force

In April 2020, the Management Committee designated a Task Force composed of Corporate Risk Owners to guide the analysis of the global risks brought by the pandemic in-line with the Secretary General’s six Strategic Focus Areas and to lead the implementation of risk mitigation strategies.

As part of its responsibilities and deliverables, the Task Force guides the efforts of the Secretariat as follows:

(i) Preparing a detailed analysis pertaining to the Strategic Focus Areas identified by the Secretary-General;
(ii) Reviewing the Secretariat-wide Risk Register in the context of the pandemic and ensuring this is detailed and explicit enough to provide a guide to action to the Corporate Risk Owners;
(iii) Preparing a simplified Secretariat-wide Risk Register for senior managers; and
(iv) Ensuring the linkage between the two levels: the overarching priorities of the Secretary-General and the Secretariat-wide Risk Register.
Moreover, the Task Force:

(v) Provides advice and guidance in the development and maintenance of the Secretariat-wide Risk Register and Risk Treatment and Response Plans on high-level risks on which the Organization should concentrate its efforts, under the leadership of the respective Corporate Risk Owners;

(vi) Brings their specific experience and expertise to ERM implementation as necessary;

(vii) Monitors the overall risk profile of the Organization and the progress of the corporate risk owners in the implementation of risk mitigation actions; and

(viii) Periodically advises the Management Committee, as the Enterprise Risk Management Committee for the Secretariat, on progress and on future actions for the implementation of ERM in the Organization.

**Corporate Risk Owners**

Corporate Risk Owners are responsible for ensuring that risks under their responsibility have been appropriately identified and that risk mitigation strategies have been brought to the attention of the Management Committee Task Force on ERM.

In these functions, they:

(i) Chair and lead the discussion of Risk Treatment and Response Working Groups;

(ii) Coordinate the preparation of Risk Treatment and Response Plans based on the inputs of the dedicated Working Groups and periodically (quarterly) report to the Management Committee on risk response implementation;

(iii) Assess the effectiveness of established controls; and

(iv) Bring to the attention of the Management Committee Task Force on ERM any emerging issues that might arise during the process.

**Heads of Entities**

Under the Secretary General’s recently adopted management paradigm, responsibility for the effective implementation of risk management practices, as described by this framework, resides with the respective heads of entities.

As part of the updated Senior Managers’ compacts with the Secretary-General, all heads of entities shall undertake strategic planning based on risk assessment and highlight key risks, and annually confirm their responsibilities for the proper application of the principles and requirements of this framework, and the establishment and maintenance of a strong internal control environment as a result of the risk assessment process.

Further responsibilities include:

(i) Properly considering the entity’s mandate in identification of relevant risks and strategies and implementing a risk management process following the guidelines of the ERM framework;
(ii) Ensuring that risks are correctly identified, managed and monitored, and duly considered in the planning and budgeting process;

(iii) Implementing appropriate risk monitoring and risk treatment plans;

(iv) Providing full support with regard to the implementation of effective risk management and internal control practices, whilst delegating appropriate responsibility for risk and internal control management in accordance with the guidelines established by the framework, and supporting policies and procedures;

(v) Reviewing and approving the risk management reports for their area of responsibility, and identifying and reporting significant and emerging risks to the Management Committee, and the Secretary-General; and

(vi) Developing adequate risk management expertise in their respective areas, ensuring proper participation to relevant training activities.

**Local Enterprise Risk Management Committees**

Without the need of creating separate structures or bodies, at the level of each Entity, the Senior Management Team naturally assumes the role of *Local ERM Committee*, embedding ERM in already established managerial mechanisms. The Committee provides overall guidance and direction regarding the implementation of ERM in the department or office, *quarterly reviews* the local risk profile and the adequacy of risk response strategies and provides relevant advice to the head of entity and risk owners. Annex 5 shows terms of reference, composition, frequency of meetings and quorum requirements for local Risk Management Committees.

**Local Risk Management Focal Points**

Local Risk Management focal points are responsible for undertaking and coordinating local risk assessments at the entity level. They are expected to review the progress of the risk assessment, the local level risk register and emerging risks to their operations on a regular basis, as well as take actions to develop and implement risk treatment and response plans to mitigate critical risks.

Local Risk Management Focal Points have been formally appointed by heads of each entity, with reporting lines to their local management, while liaising with the ERM function in DMSPC to support the implementation of risk assessment and risk and internal control monitoring activities. Responsibilities have been assigned to one or more existing staff, on a full-time or part-time basis, as deemed suitable by the responsible management considering the complexities of the underlying operations.

More specifically, the responsibilities of local Risk Management Focal Points include the provision of assistance to local management in the implementation of the risk management requirements described by this framework, in particular the identification of relevant risks, based on the objectives and mandates of the relevant entity; the completion of the risk assessment and reporting on its results; the definition of the activities that should be included in the Risk Treatment and Response Plan; and undertaking monitoring and reporting to senior management on risk management and internal control measures within their area of responsibility.
In addition, local Risk and Internal Control Focal Points shall customise the Secretariat-wide Risk Universe so that it reflects the risks relevant to the entity; prepare reports on all risk management matters and distribute them to the Enterprise Risk Management function in DMSPC, and the responsible head of entity and local ERM Committee; and monitor the effectiveness of risk management and internal control measures.

**Risk Owners and Risk Treatment Owners**

Risk owners are responsible, amongst other matters, for:

(i) Regularly reviewing the risks owned by them, informing the local Risk Management Focal Points of any identified changes, and escalating the risks for which the relevant impact or likelihood is perceived to have increased.

(ii) Determining where internal control deficiencies relating to their risks may be identified, proposing any appropriate risk mitigation measures, and monitoring implementation of risk treatment and response plans relating to risks for which they have responsibility.

(iii) Updating relevant risk information and contributing to risk reporting as may be required.

**Risk Treatment Working Groups**

Risk Owners could be supported in their responsibilities by dedicated working groups comprised of thematic experts from across the Organization or entity, as deemed appropriate by the ERM Committee. The Working Groups, through periodic discussions, will:

(i) Revise the key drivers, the proposed controls and the risk responses.

(ii) Contribute to the definition of Risk Treatment and Response Plans and their implementation under the supervision of the Risk Owners; and

(iii) Bring to the attention of the Risk Owners any emerging issues that might arise during the process.

**Enterprise Risk Management Section in the Department of Management Strategy, Policy and Compliance**

Enterprise risk management is the inherent core responsibility of management. Under the framework, embedded risk and internal control management activities are an integral part of the processes and operations of the entire Organization.

Following the Secretary-General’s Management reform, the formerly established Enterprise Risk Management function has been reinforced in the Business Transformation and Accountability Division of the Department of Management Strategy, Policy and Compliance (DMSPC) to assist senior management in the process of implementation of the framework. According to best practices and in line with the JIU recommended benchmarks\(^6\), as well as the non-prescriptive

---

\(^6\) Paragraph 24, JIU/REP/2020
guidelines developed by the High-Level Committee on Management (HLCM) taskforce on ERM, the ERM function strives to integrate ERM in the programme planning processes.

As management is the owner of the identified risks, the ERM section facilitates the effective implementation of the ERM framework. It provides assistance to different entities in implementing risk management based on systematic risk mitigation strategies consistently applied across the Secretariat, aggregating risk data from the different organizational units and offices and carrying out regular monitoring of UN Secretariat-wide risks.

The ERM section shall as well facilitate the adoption of consistent methodologies for the assessment of risks throughout United Nations Secretariat, and the implementation of enhanced internal control and risk mitigation measures at the entity level, cooperating with dedicated Risk Focal Points. This process will enable the UN Secretariat to aggregate related risk and internal control data across the Organization and design the optimal strategies to address the most significant risks to which the UN Secretariat is exposed.

In detail, the main responsibilities of the ERM function in DMSPC include:

(i) Promoting the application of sound risk management policies and providing oversight for the implementation of related activities within the UN Secretariat, defining an overall vision and direction for ERM activities.

(ii) Defining a comprehensive ERM framework across the Organization to identify, assess, manage and monitor risks and internal controls, supporting the Secretary-General and management in their efforts to embed and sustain risk management activities in the daily operations of the Secretariat.

(iii) Maintaining the Secretariat-wide Risk Register, introducing enhancements over time, and coordinating the performance of the risk assessment, holding interviews, developing and reviewing questionnaires, and facilitating workshops, as may be needed.

(iv) Providing the necessary expertise and resources to support the different steps in the risk management process, including assistance and advisory in the design, assessment, and monitoring of appropriate risk mitigation activities and formal Risk Treatment and Response Plans.

(v) Developing and maintaining the methodology and practices related to the implementation of risk management activities, including the administration of the tools, training, reporting and other related requirements, and supporting the local Risk Management Focal Points in conducting appropriate risk and internal control monitoring activities.

(vi) Preparing reports on risk management activities for distribution to the Management Committee, Secretary-General, and on behalf of the Secretary-General to the General Assembly and the IAAC, as may be required.

(vii) Assisting in the provision of monitoring and oversight of risk management at the entity level, and advising as appropriate on the development and maintenance of local Risk Registers and local Risk Treatment and Response Plans.

---

(viii) Implementing and maintaining the necessary information technology (IT) solutions and data management capabilities to properly support the risk management across the Secretariat entities.

(ix) Supporting the dissemination of information and best practices regarding risk management principles and measures across the Secretariat, and developing as appropriate communication and training programs, including websites, e-learning courses and communities of practice, to enhance the Secretariat’s risk management culture.

(x) Attending the meetings of the Risk Treatment Working Groups to be held under the leadership of Corporate Risk Owners for the Secretariat-wide Risk Register.

**Management and Staff Members**

The management of risks and internal controls in accordance with the principles defined by the ERM Policy of the Organization is the responsibility of all UN managers and staff members. Defined responsibilities, that will depend on the specific role and function, broadly include:

(i) Embedding risk management in strategic and operational decision making, identifying, managing and monitoring risks with regard to day-to-day operations within the areas of responsibility.

(ii) Providing oversight on the appropriate application of risk management methodologies by the staff members reporting to them, where relevant.

(iii) Monitoring the efficiency and effectiveness of defined control and risk mitigation measures, and contributing to the planning and budgeting process with regard to risk management matters, if applicable.

(iv) Escalating risks as it may be appropriate and providing timely and accurate risk information to Risk Owners, Risk Focal Points, and the ERM function.

(v) Providing visible support to the implementation of the Secretariat’s ERM framework.
Office of Internal Oversight Services

In accordance with its mandate, the Office of Internal Oversight Services shall continue to be responsible for evaluating the effectiveness of the internal control environment, including the periodic assessment and evaluation of the implementation of an effective ERM framework.

The Office of Internal Oversight Services is as well responsible for the review of the results of the risk assessments process and shall consider its outcomes into its audit planning exercise, as deemed appropriate.

Joint Inspection Unit

The Joint Inspection Unit, as the oversight body of the United Nations system mandated to conduct system-wide evaluations, shall identify enterprise risk management and internal control best practices, propose benchmarks, and facilitate information-sharing throughout the system.

Board of Auditors

The Board of Auditors, as part of its assurance activities on the financial reporting of the Organization, is expected to utilise the results of the risk assessment as an important element of its evaluation of the Organization’s system of internal controls, as described by its mandate.
## Annexes

<table>
<thead>
<tr>
<th>Annex</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annex 1</td>
<td>United Nations Secretariat Risk Universe</td>
<td>39</td>
</tr>
<tr>
<td>Annex 2</td>
<td>Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control Effectiveness</td>
<td>40</td>
</tr>
<tr>
<td>Annex 3</td>
<td>Glossary of Terms and Definitions</td>
<td>42</td>
</tr>
<tr>
<td>Annex 4</td>
<td>Risk Assessment Interview Sample Questionnaire</td>
<td>44</td>
</tr>
<tr>
<td>Annex 5</td>
<td>Risk Management Committee Generic Terms of Reference</td>
<td>46</td>
</tr>
<tr>
<td>Annex 6</td>
<td>Annual Enterprise Risk Management Reporting Template</td>
<td>47</td>
</tr>
</tbody>
</table>
### Annex 1. United Nations Secretariat Risk Universe

#### Strategic
- **1. Planning**
  - 1.1 Vision and Mandate
  - 1.2 Strategic Planning
  - 1.3 Budgeting
  - 1.4 Budget Allocation
  - 1.5 Result Performance Measurement
  - 1.6 Planning Execution & Integration
  - 1.7 HR Strategy and Planning
  - 1.8 Organizational Synchronization
  - 1.9 Outsourcing
  - 1.10 Org. Transf & Mgmt Reform

#### Governance
- **2.1 Governance**
  - 2.1.1 Tone at the Top
  - 2.1.2 Control Environment/ Risk Mgmt
  - 2.1.3 Organizational Structure
  - 2.1.4 Transparency
  - 2.1.5 Accountability
  - 2.1.6 Empowerment

#### Ethical behaviour
- **2.2 Ethical behaviour**
  - 2.2.1 Ethics
  - 2.2.2 Sexual exploitation and Abuse
  - 2.2.3 Professional Conduct
  - 2.2.4 Sexual Harassment

#### Internal & External Factors
- **3.1 Internal & External Factors**
  - 3.1.1 Political Climate - Internal
  - 3.1.2 Economic Factors - Commodity
  - 3.1.3 Unprecedented Events (i.e. Pandemic)
  - 3.1.4 Climate Change

#### Reputation
- **4.1 Reputation**
  - 4.1.1 Public Perception & Reputation
  - 4.1.2 Crisis & Contingency Mgmt

#### Financial
- **5.1 Financial**
  - 5.1.1 Financial Contributions
  - 5.1.2 ICT Governance & Cyber Security
  - 5.1.3 Umost System Control Environment

#### Fraud & Corruption
- **6.1 Fraud & Corruption**
  - 6.1.1 Organizational Culture & Environment
  - 6.1.2 ICT Governance & Cyber Security
  - 6.1.3 Umost System Control Environment

#### Human Resources
- **7.1 Human Resources**
  - 7.1.1 Educational/Professional Cred
  - 7.1.2 Financial Controls
  - 7.1.3 Payroll, Attendance, Travel, Leave

#### Central Services
- **8.1 Central Services**
  - 8.1.1 Procurement
  - 8.1.2 Procurement Services & Support

#### Compliance
- **9.1 Compliance**
  - 9.1.1 Procurement
  - 9.1.2 Procurement Services & Support
# Annex 2. Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control Effectiveness

## Impact

<table>
<thead>
<tr>
<th>Score</th>
<th>Rating</th>
<th>Safety and security</th>
<th>Duration</th>
<th>Organizational and operational scope</th>
<th>Reputational impact</th>
<th>Impact on operations</th>
<th>Financial impact (measured in terms of budget)</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Critical</td>
<td>Loss of life (staff, partners, general population)</td>
<td>Potentially irrecoverable impact</td>
<td>Organization-wide: inability to continue normal business operations across the Organization.</td>
<td>Reports in key international media for more than one week</td>
<td>Inability to perform mission or operations for more than one month</td>
<td>&gt;5 per cent $&gt;500 million</td>
<td>Requires significant attention and intervention from General Assembly and Member States</td>
</tr>
<tr>
<td>4</td>
<td>Significant</td>
<td>Loss of life due to accidents/ non-hostile activities</td>
<td>Recoverable in the long term (i.e., 24-36 months)</td>
<td>Two (2) or more departments/offices or locations: significant, ongoing interruptions to business operations within 2 or more departments/offices or locations</td>
<td>Comments in international media/forum</td>
<td>Disruption in operations for one week or longer</td>
<td>3-5 per cent $300 million-$500 million</td>
<td>Requires attention from senior management</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
<td>Injury to United Nations staff, partners and general population</td>
<td>Recoverable in the short term (i.e., &lt;12 months)</td>
<td>One (1) or more departments/offices or locations: moderate impact within one or more departments/offices or locations</td>
<td>Several external comments within a country</td>
<td>Disruption in operations for less than one week</td>
<td>&lt;2-3 per cent $200 million-$300 million</td>
<td>Requires intervention from middle management</td>
</tr>
<tr>
<td>2</td>
<td>Moderate</td>
<td>Loss of infrastructure, equipment or other assets</td>
<td>Temporary (i.e., &lt;12 months)</td>
<td>One (1) department/office or location: limited impact within department/office or location</td>
<td>Isolated external comments within a country</td>
<td>Moderate disruption to operations</td>
<td>&lt;1-2 per cent $100 million-$200 million</td>
<td>Issues delegated to junior management and staff to resolve</td>
</tr>
<tr>
<td>1</td>
<td>Low</td>
<td>Damage to infrastructure, equipment or other assets</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
<td>Not applicable or limited impact</td>
</tr>
</tbody>
</table>
### Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control Effectiveness

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Score</th>
<th>Rating</th>
<th>Certainty</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>Expected</td>
<td>&gt;90 per cent</td>
<td>At least yearly and/or multiple occurrences within the year</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Highly likely</td>
<td>&lt;90 per cent</td>
<td>Approximately every 1-3 years</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Likely</td>
<td>&lt;60 per cent</td>
<td>Approximately every 3-7 years</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Unlikely</td>
<td>&lt;30 per cent</td>
<td>Approximately every 7-10 years</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Rare</td>
<td>&lt;10 per cent</td>
<td>Every 10 years and beyond or rarely</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level of Internal Control / Management Effectiveness</th>
<th>Score</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5</td>
<td>Effective</td>
<td>Controls are properly designed and operating as intended. Management activities are effective in managing and mitigating risks</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>Limited improvement needed</td>
<td>Controls and/or management activities are properly designed and operating somewhat effectively, with some opportunities for improvement identified</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Significant improvement needed</td>
<td>Key controls and/or management activities in place, with significant opportunities for improvement identified</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Ineffective</td>
<td>Limited controls and/or management activities are in place, high level of risk remains. Controls and/or management activities are designed and are somewhat ineffective in efficiently mitigating risk or driving efficiency</td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>Highly ineffective</td>
<td>Controls and/or management activities are non-existent or have major deficiencies and do not operate as intended. Controls and/or management activities as designed are highly ineffective in efficiently mitigating risk or driving efficiency</td>
</tr>
</tbody>
</table>
### Annex 3. Glossary of Terms and Definitions

<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Effectiveness</td>
<td>A measure of how reliably the internal control operates.</td>
</tr>
<tr>
<td>Enterprise Risk Management</td>
<td>The process of coordinated activities designed to direct and control an organization with regard to risk, the effect of uncertainty on objectives. It is effected by governing bodies, management and other personnel, and applied in strategy-setting throughout the Organization. Internal control is encompassed within and an integral part of enterprise risk management.</td>
</tr>
<tr>
<td>Internal Control</td>
<td>A process, effected by governing bodies, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.</td>
</tr>
<tr>
<td>Impact</td>
<td>Result or effect of an event. There may be a range of possible impacts associated with an event. The impact of an event can be positive or negative relative to the entity’s related objectives.</td>
</tr>
<tr>
<td>Largest Credible Risk</td>
<td>Risk Exposure in the case of simultaneous failure of several controls established to mitigate the risk.</td>
</tr>
<tr>
<td>Likelihood</td>
<td>The possibility that a given event will occur.</td>
</tr>
<tr>
<td>Reasonable assurance</td>
<td>The concept that enterprise risk management, even if well designed and operated, cannot provide a guarantee regarding the achievement of an entity’s objectives, due to the limitations of the human judgement; resource constraints and the need to consider the cost of controls in relation to expected benefits; and the possibility of management override and collusion.</td>
</tr>
<tr>
<td>Residual Risk</td>
<td>The remaining risk after management has taken action to alter the risk’s likelihood or impact.</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residual Risk Heat Map</td>
<td>Risk Exposure and Internal Control Effectiveness Matrix – Overview of the Organization’s main risks. Typically, a four or multi-quadrant chart is used to display risk assessment results, as a function of Risk Exposure and Level of Risk Mitigation Activities or Internal Control Effectiveness.</td>
</tr>
<tr>
<td>Risk</td>
<td>The effect of uncertainty on objectives.</td>
</tr>
<tr>
<td>Risk Appetite</td>
<td>Risk Appetite can be defined as the aggregate amount of risk an organisation seeks to assume in pursuit of its strategic objectives and mission.</td>
</tr>
<tr>
<td>Risk Dashboard</td>
<td>Summary of the significant risks identified as a result of the risk assessment process. Composite of the risks that have been assessed to the most important to the Organization.</td>
</tr>
<tr>
<td>Risk Exposure</td>
<td>Magnitude of a risk measured in terms of the combination of Impact and Likelihood.</td>
</tr>
<tr>
<td>Risk Register</td>
<td>Central repository of all risks and risk information maintained by the Organization, including the risk category, sub-category, risk, risk definition, rating results, contributing factors, and other relevant information pertaining to that risk.</td>
</tr>
<tr>
<td>Risk Tolerance</td>
<td>Acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives; or put another way the boundaries of risk taking outside of which the organisation is not prepared to venture in the pursuit of its long-term objectives.</td>
</tr>
<tr>
<td>Risk Universe, or Risk Catalogue</td>
<td>High level description of all the risks relevant to the Organization, including the risk category, sub-category, risk and risk definition.</td>
</tr>
<tr>
<td>Tier 1 Risks</td>
<td>Very High Risks – Risks perceived to be of greatest importance based on relative level of significance to the Organization and location, and that require the most attention.</td>
</tr>
<tr>
<td>Tier 2 Risks</td>
<td>High Risks – Risks which may require dedicated focus and specific remedial action.</td>
</tr>
<tr>
<td>Tier 3 Risks</td>
<td>Medium Risks – Other risks determined to have a medium exposure, and that might require specific remedial or monitoring measures.</td>
</tr>
</tbody>
</table>
Annex 4. Risk Assessment Interview Sample Questionnaire

One-on-one interviews with members of the senior management team are an effective and powerful tool to gather information. By linking risks to strategic objectives, they can be an excellent vehicle to collect information related to risks and a unique source of meaningful discussions.

The interviews, which should be of confidential nature, are facilitated by the ERM function or the local department or office ERM focal point(s) and require a quite high level of tact and interviewing skills. It would be ideal if the ERM team could be represented by two colleagues, if at all possible, one leading the conversation, the other taking detailed notes.

Background (provided by the ERM team)

1. Provide a brief background on what ERM is and how it can add value to the work of the department and unit.

2. Briefly describe the mandate, objectives, scope and the risk assessment process.

3. If needed, refer to the relevant objectives of the office or department for the period under consideration.

4. Present the existing risk register (if applicable) or the draft risk register emerging from the initial desk review, as well as the preliminary risk dashboard.

   Providing a visual representation of the preliminary dashboard (as presented in Figure 4 of this document) might help guide the discussion.

5. Confirm the confidential nature of the interview, as input will be consolidated and included in the risk register with no reference that could identify the source of the information.

Interview (questions to the interviewee)

6. Briefly describe the objectives and operations for your area of responsibility.

7. Considering those specific objectives, outline what are the main risks (approx. 1 to 3) which could have an impact on your ability to achieve them. Elaborate on their root causes, drivers, and the existing controls.

8. Considering the preliminary risk dashboard emerging from the desk review, identify the most critical risks (3 to 5) to the objectives of the wider office or department.

9. For each mentioned risk, elaborate on (i) root causes and drivers, and (ii) existing controls (if appropriate, focus on understanding the implied level of impact, likelihood and control effectiveness, based on the pre-defined assessment criteria).

   Personalities might be quite different. Every manager brings to the conversation their individual approach and perspective, and the difference in perspectives represents an important value in itself to the risk assessment process. Some managers might limit to touching the high level most strategic risks, without providing an opinion on risk ratings.
and relevant trends, other might have a much more analytical approach and describe in detail risk areas, related drivers and the effectiveness of designed controls and managerial responses.

The ERM team should support them during the discussions, tailoring follow-up questions and clarifications to the managerial style of the interviewee and of course to the specific nature of observations and risks. This is the less structured part of the interview, as it should logically follow the direction of the conversation. Of course, the underlying objective of the ERM team would continue to be the understanding the level of impact and likelihood of risks and the effectiveness of existing controls, based on the pre-defined assessment criteria.

10. Considering the effectiveness of existing measures and controls, for each risk identify which additional measures the Organization or department might take to reduce exposure: i.e., what could be the risk response strategy and action plan.

11. Consider whether other risks not already identified as part of the initial risk dashboard could impact the achievement of objectives, if any. In case further risk areas emerge, elaborate on (i) root causes and drivers, and (ii) existing controls.

Conclusion (provided by the ERM team)

12. Recognise the time and efforts of the interviewee in the process, and the value of their contribution and experience.

13. Outline the next steps in the assessment process, and in particular the subsequent validation of identified risks in a wider workshop were all the different parties (including the interviewees) will discuss the preliminary risk register, emerging as a summary of the individual contributions up to that point, and find a consensus on risk areas, their priorities, risk ownership, and a way forward on risk treatment and response plans.
Annex 5. Local Risk Management Committee Generic Terms of Reference

Mandate

In accordance with the Secretariat’s Enterprise Risk Management policy, head of entities are responsible for the effective implementation of risk management practices in their areas of responsibility. They shall constitute a Local Risk Management Committee, in particular in Peacekeeping Missions, with representation from across the entity to align and coordinate activities related to risk management matters.

The Committee shall serve as a forum to build consensus on key strategic areas by validating and prioritizing risks; identifying trends and emerging risks; and reviewing and recommending measures to proactively manage risks.

Functions of the Local Risk Management Committee

Reporting to the head of entity, the Committee will perform the following functions:

(i) Validate and prioritize risks identified across the entity and determine the risks to be reflected in the risk register;
(ii) Ensure the alignment of the risk management framework with the Secretariat-wide Policy and Methodology;
(iii) Review the final Risk Register prior to submission for approval to the head of entity;
(iv) Perform ongoing reviews and updates of the Risk Register and identify emerging risks, and determine the risks to be added or downgraded from the risk register;
(v) Submit the consolidated plan of risk treatment measures to the head of entity;
(vi) Deal with any other relevant risk management and internal control matters.

Composition

The local ERM committee shall be composed of the Senior Leadership/Management team of each entity, including the local Risk Management focal point(s) as the secretariat of the Committee.

Frequency of meetings and Quorum

The Committee shall meet at least quarterly to assess and validate risks and review the adequacy and effectiveness of risk mitigation measures as detailed in the consolidated risk treatment plan.

A meeting shall be considered as duly constituted when majority of the members are present.

The Committee shall maintain a written record of the main issues and recommendations discussed during the meeting.
Annex 6. Annual Enterprise Risk Management Reporting Template

Entity Name: ……. / For the year ending (Day) (Month) 20____

1. **Purpose**: Reporting annually to the USG/DMSPC on the progress of the implementation of ERM and on the results of deliberations of local ERM Committee regarding the top risks identified and the mitigation strategies in place.

2. **Enterprise Risk management (ERM) capacity**:
   
   2.1 There are ______ positions currently assigned to ERM in the Entity.
   
   2.2 Reporting lines on ERM are as follows: ______
   
   2.3 Remarks on the effectiveness of the reporting lines: ______

3. **Implementation of ERM**:
   
   3.1 Has the Entity established a **Risk Register**? Yes___ No___.
   
   *If yes, please attach a copy of the Risk register to this report.*
   
   *If no, what is your timeline for establishment of one? All entities must have a risk register by 31 December 2023.*
   
   3.2 Has the Entity developed **Risk Treatment and Response Plans**? Yes___ No___.
   
   *If yes, please attach a copy of the Risk Treatment and Response Plans including the status of implementation.*
   
   3.3 Has the Entity established a local **Enterprise Risk Management Committee** (ERMC)? Yes___ No___.
   
   *Please provide details of its membership and reporting lines.*

4. **Certification**

   I, _____________ (name), ___________ (title), hereby certify that all data transmitted in the present report is valid, accurate and fully represents the status of ERM in (Entity acronym).

   Signature  ______________________

   Date  ______________________