UNITED NATIONS NATIONS UNIES

Enterprise Risk Management and Internal Control Methodology

May 2011

Table of Contents

Annexes

Enterprise Risk Management and Internal Control Methodology

I. Background

Whilst risk management is an area already considered at various levels, and embedded in different processes and operations of the United Nations Secretariat, departments and programmes have developed their own methodology, adopting one of the several different risk management standards currently available, and have employed a diverse range of processes to identify, evaluate and respond to risks, so that each area focuses on risk and risk management activities in a different manner. As a result, the processes in place are not aligned with one another, and do not share a consistent methodology for identifying, evaluating, responding to, and reporting risks. The possibility to effectively draw on the risk information currently available appears therefore extremely limited.

At the same time, the Secretariat faces a considerable level of risks inherent to its operations, due to the complexities and increased scope of its mandates. Some of those underlying risks may also be difficult to identify, as the execution of the mandates involves multiple entities, internal and external to the Organization. Accordingly, promoting a systematic risk-based approach to management decisions and risk mitigation becomes critical.

Building on the expertise of relevant United Nations entities and oversight bodies, this document outlines an enterprise risk management methodology that is applicable across the entire Organization.

II. Purpose

With the adoption of an enterprise risk management and internal control process as a strategic initiative, the Secretariat will define a consistent methodology for assessing, monitoring and communicating risks. The Enterprise Risk Management and Internal Control Framework ("the framework"), as described by this Methodology, will effectively address both the strategic risks associated with the execution of the mandates and objectives as defined by the Charter of the United Nations, as well as the risks inherent in the daily operations that support the achievement of those mandates. The implementation of this framework is designed to introduce significant enhancements in the governance and management practices of the Organization, some of which are 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, and the systematic measurement of risk and performance.

(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 tradeoffs 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.

III. Definition

Consistent with the best international standards[1] enterprise risk management 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.

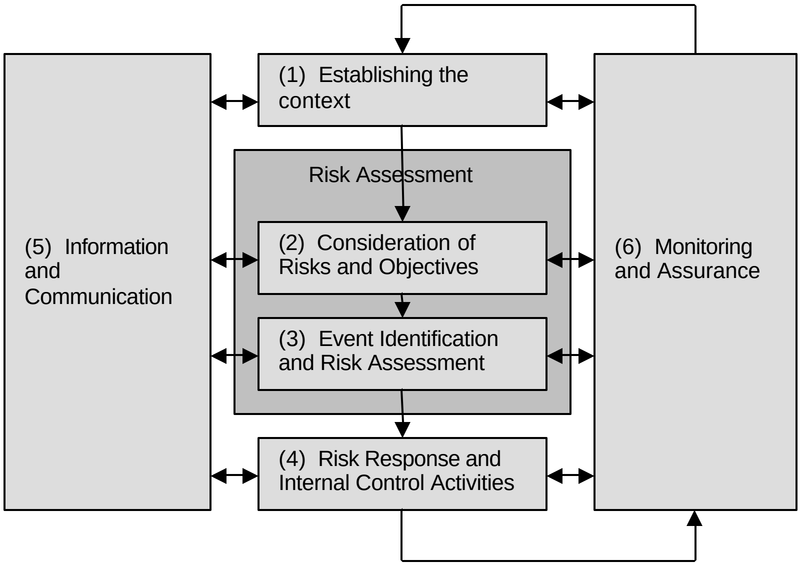
Accordingly, an effective system of internal control is encompassed within and an integral part of enterprise risk management. As defined by the best international standards, enterprise risk management is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualisation and tool for management.

[1] "Enterprise Risk Management - Integrated Framework" and "Thought Papers on Enterprise Risk Management", Committee of Sponsoring Organizations of the Treadway Commission, 2004, 2009, 2010 and 2011;
"Guidelines for Internal Control Standards for the Public Sector", Internal Control Standards Committee of the International Organization of Supreme Audit Institutions, 2004 and 2007; and
"Risk management – Principles and Guidelines" – International Organization for Standardization, 2009.

IV. Enterprise Risk Management and Internal Control Framework

Enterprise Risk Management is a process owned and executed by management. The main components of the risk management process are illustrated in Figure 1 below, and further described in this section of the document. The definition of all the relevant technical terms is included in Annex 4 of this Methodology – Glossary of Terms and Definitions.

Figure 1 - Enterprise Risk Management and Internal Control Process


(1) Establishing the context
Risk Assessment
(2) Consideration of Risks and Objectives
(3) Event Identification and Risk Assessment
(4) Risk Response and Internal Control Activities
(5) Information and Communication
(6) Monitoring and Assurance

In particular:

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

(2) **Consideration of Risks and Objectives** – Risks shall be mapped and aligned to objectives, mandates and strategic initiatives at both the UN Secretariat and functional level (Departments, Offices, Commissions, Missions and Tribunals) in order to measure and prioritise the inherent risks. Specific measurement criteria for risk evaluation shall be as well defined.

(3) **Event Identification and Risk Assessment** – Risks are assessed in the context of the objectives, mandates and strategic plans through risk questionnaires, interviews, workshops with relevant management and staff, and other sources. Identified risks shall then be measured and scored according to the perceived impact, likelihood and level of internal control effectiveness.

(4) **Risk Response and Internal Control Activities** – Risks shall be prioritised at first based on the overall ratings for each risk in terms of inherent 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 shall

be determined based on the overall risk prioritisation, and implemented in accordance with defined procedures. 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, shall be established. Appropriate communication and training programs shall be 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 shall be as well implemented.

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

IV.1 Establishing the Context

As a preliminary step in the process of implementation of a comprehensive framework, the Organization shall adopt an overall Enterprise Risk Management and Internal Control Policy ("the Policy"), articulating the purpose, governance mechanisms, and principles that will guide the adoption of the framework. The Policy shall be individually applied to the different Departments according to the level and context of risk and risk assessment. The principles established by the Policy that complements this Methodology are described below.

Principles

The enterprise risk management 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 organizational unit, and the Secretariat at entity level.

(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 enterprise risk management 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 in particular be integrated with the adoption of an effective results based management approach. Enterprise risk management 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 be also fully considered in the evaluation of programmes and relevant budget allocations.

The effective implementation of the framework within the Secretariat shall rely 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 with regard to 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 shall therefore be 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 each level throughout the Organization for risk management and internal control activities.

(iii) **Resources** – Risk and internal control management shall be supported by adequate resources, at Department, Office, Commission, Mission and Tribunal level, as well as at entity level.

IV.2 Consideration of Risks and Objectives

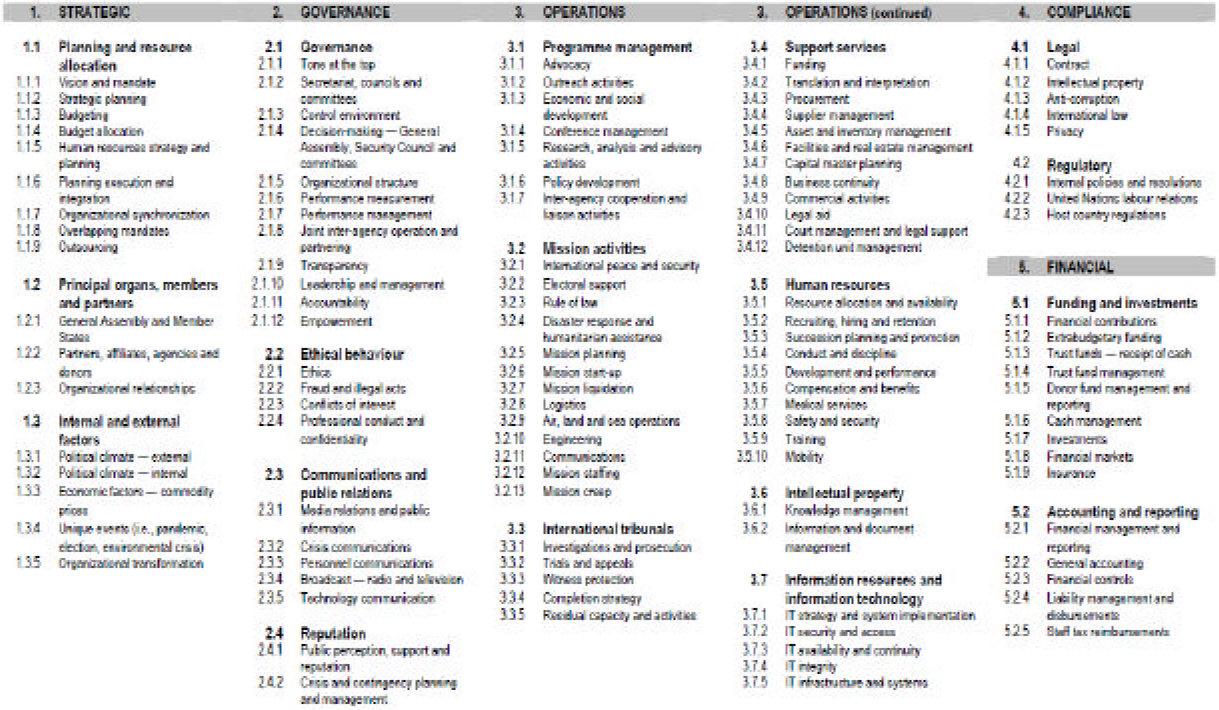
The initial stages of the risk assessment process require the alignment and mapping of risks to the underlying strategies, plans and objectives, to better measure and prioritise the risks inherent in each, and the required risk management and risk treatments activities designed to effectively mitigate those risks.

It becomes therefore crucial to describe the risks that are relevant for further consideration based on the established risk management framework, starting with the definition of the Secretariat's Risk Catalogue, or Risk Universe, as the basis for the completion of all the detailed risk assessments. The defined Risk Universe, attached to this Methodology as Annex 1, represents a high level description of all of the risks relevant to the Organization, and shall be then tailored, as required, to reflect the profile of the organizational unit under consideration. Each Department, Office, Commission, Mission and Tribunal 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 entity level Risk Universe created for the Secretariat.

The Organization will this way adopt a common risk language, allowing the Secretariat to collect and appraise risk information on multiple levels across the overall 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 a system-wide basis, as well as to assess the overall effectiveness of existing internal controls and measures of risk mitigation.

The Risk Universe for the Secretariat, that was developed by management in 2008 with the advice of a consulting firm, identifies and defines a catalogue of 116 risks, categorized into five major risk areas: (1) Strategic, (2) Governance, (3) Operational, (4) Compliance, and (5) Financial risks.

Figure 2 – United Nations Secretariat Risk Universe *(Annex 1)*



1.	**STRATEGIC**
1.1	**Planning and resource allocation**
1.1.1	Vision and mandate
1.1.2	Strategic planning
1.1.3	Budgeting
1.1.4	Budget allocation
1.1.5	Human resources strategy and planning
1.1.6	Planning execution and integration
1.1.7	Organizational synchronization
1.1.8	Overlapping mandates
1.1.9	Outsourcing
1.2	**Principal organs, members and partners**
1.2.1	General Assembly and Member States
1.2.2	Partners, affiliates, agencies and donors
1.2.3	Organizational relationships
1.3	**Internal and external factors**
1.3.1	Political climate — external
1.3.2	Political climate — internal
1.3.3	Economic factors — commodity prices
1.3.4	Unique events (i.e., pandemic, election, environmental crisis)
1.3.5	Organizational transformation
2.	**GOVERNANCE**
2.1	**Governance**
2.1.1	Tone at the top
2.1.2	Secretariat, councils and committees
2.1.3	Control environment
2.1.4	Decision-making — General Assembly, Security Council and committees
2.1.5	Organizational structure
2.1.6	Performance measurement
2.1.7	Performance management
2.1.8	Joint inter-agency operation and partnering
2.1.9	Transparency
2.1.10	Leadership and management
2.1.11	Accountability
2.1.12	Empowerment
2.2	**Ethical behaviour**
2.2.1	Ethics
2.2.2	Fraud and illegal acts
2.2.3	Conflicts of interest
2.2.4	Professional conduct and confidentiality
2.3	**Communications and public relations**
2.3.1	Media relations and public information
2.3.2	Crisis communications
2.3.3	Personnel communications
2.3.4	Broadcast — radio and television
2.3.5	Technology communication
2.4	**Reputation**
2.4.1	Public perception, support and reputation
2.4.2	Crisis and contingency planning and management
3.	**OPERATIONS**
3.1	**Programme management**
3.1.1	Advocacy
3.1.2	Outreach activities
3.1.3	Economic and social development
3.1.4	Conference management
3.1.5	Research, analysis and advisory activities
3.1.6	Policy development
3.1.7	Inter-agency cooperation and liaison activities
3.2	**Mission activities**
3.2.1	International peace and security
3.2.2	Electoral support
3.2.3	Rule of law
3.2.4	Disaster response and humanitarian assistance
3.2.5	Mission planning
3.2.6	Mission start-up
3.2.7	Mission liquidation
3.2.8	Logistics
3.2.9	Air, land and sea operations
3.2.10	Engineering
3.2.11	Communications
3.2.12	Mission staffing
3.2.13	Mission creep
3.3	**International tribunals**
3.3.1	Investigations and prosecution
3.3.2	Trials and appeals
3.3.3	Witness protection
3.3.4	Completion strategy
3.3.5	Residual capacity and activities
3.	**OPERATIONS (continued)**
3.4	**Support services**
3.4.1	Funding
3.4.2	Translation and interpretation
3.4.3	Procurement
3.4.4	Supplier management
3.4.5	Asset and inventory management
3.4.6	Facilities and real estate management
3.4.7	Capital master planning
3.4.8	Business continuity
3.4.9	Commercial activities
3.4.10	Legal aid
3.4.11	Court management and legal support
3.4.12	Detention unit management
3.5	**Human resources**
3.5.1	Resource allocation and availability
3.5.2	Recruiting, hiring and retention
3.5.3	Succession planning and promotion
3.5.4	Conduct and discipline
3.5.5	Development and performance
3.5.6	Compensation and benefits
3.5.7	Medical services
3.5.8	Safety and security
3.5.9	Training
3.5.10	Mobility
3.6	**Intellectual property**
3.6.1	Knowledge management
3.6.2	Information and document management
3.7	**Information resources and information technology**
3.7.1	IT strategy and system implementation
3.7.2	IT security and access
3.7.3	IT availability and continuity
3.7.4	IT integrity
3.7.5	IT infrastructure and systems
4.	**COMPLIANCE**
4.1	**Legal**
4.1.1	Contract
4.1.2	Intellectual property
4.1.3	Anti-corruption
4.1.4	International law
4.1.5	Privacy
4.2	**Regulatory**
4.2.1	Internal policies and resolutions
4.2.2	United Nations labour relations
4.2.3	Host country regulations
5.	**FINANCIAL**
5.1	**Funding and investments**
5.1.1	Financial contributions
5.1.2	Extrabudgetary funding
5.1.3	Trust funds — receipt of cash
5.1.4	Trust fund management
5.1.5	Donor fund management and reporting
5.1.6	Cash management
5.1.7	Investments
5.1.8	Financial markets
5.1.9	Insurance
5.2	**Accounting and reporting**
5.2.1	Financial management and reporting
5.2.2	General accounting
5.2.3	Financial controls
5.2.4	Liability management and disbursements
5.2.5	Staff tax reimbursements

Once completed, the outcomes of the risk assessment process shall eventually be captured in the Organization's Risk Register, the central repository of all relevant risk information that will be maintained by the Organization. The Risk Register will include the Risk Universe (the risk category, sub-category, risk, and risk definition), and further information regarding rating results, and applicable contributing risk factors and drivers. Each unit location shall then maintain the relevant sub-set of risks within the Risk Register, reflecting any relevant changes in the risk environment. A comprehensive review shall be completed at least annually, as a result of the periodic risk assessment.

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.

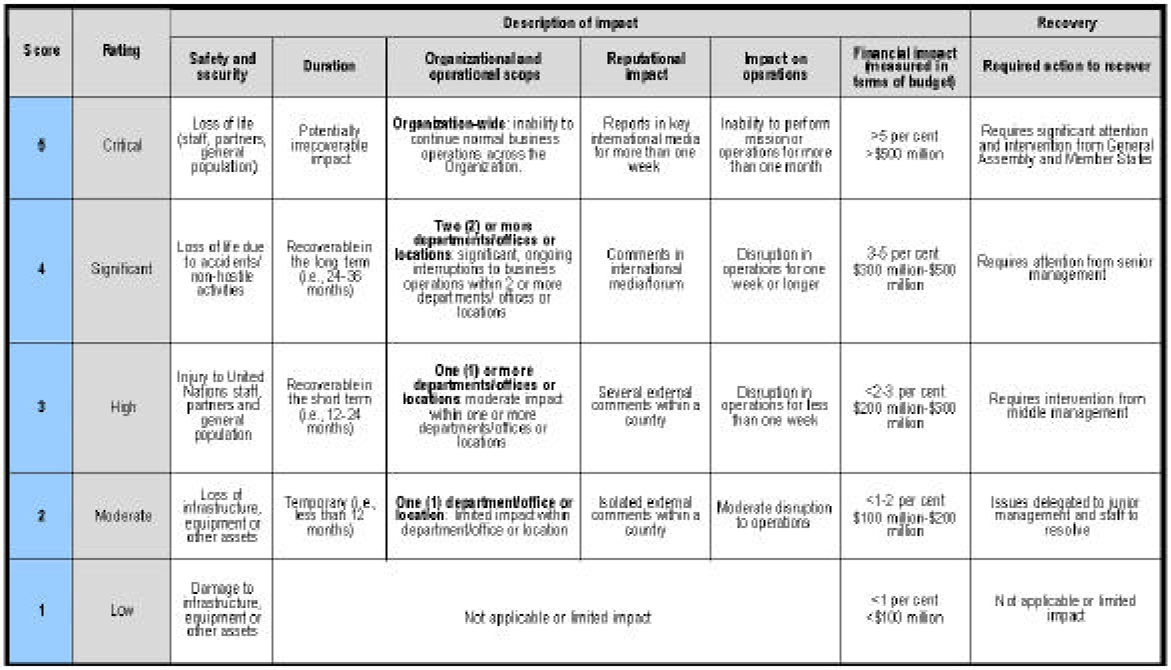
(ii) **Likelihood** – The possibility that a given event will occur.

(iii) **Internal Control 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.

Management has defined the scoring criteria for the measurement of impact, likelihood and level of control effectiveness in mitigating risk at the Secretariat entity level, as described in Annex 2 of this Methodology.

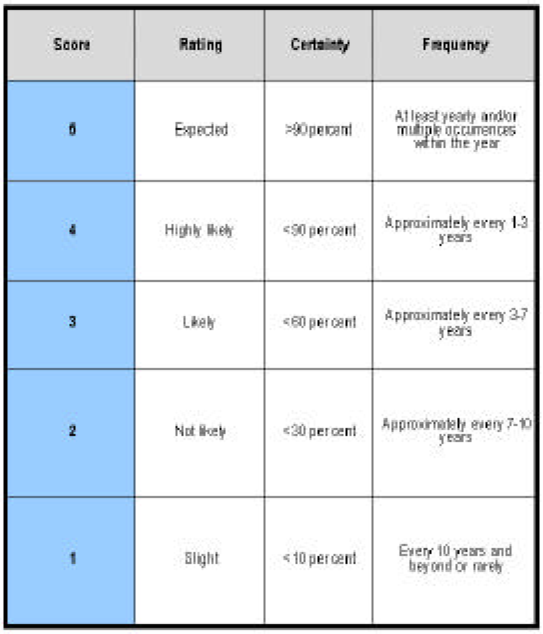
Figure 3 – Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control Effectiveness *(Annex 2)*

Impact



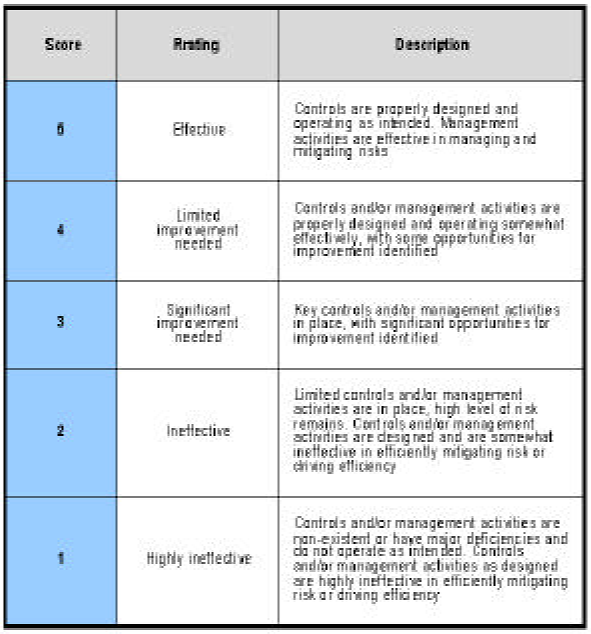
Score	Rating	Description of impact						Recovery
		Safety and security	Duration	Organizational and operational scope	Reputational impact	Impact on operations	Financial impact (measured in terms of budget)	Required action to recover
5	Critical	Loss of life (staff, partners, general population)	Potentially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

Likelihood



Score	Rating	Certainty	Frequency
5	Expected	>90 percent	At least yearly and/or multiple occurrences within the year
4	Highly likely	<90 percent	Approximately every 1-3 years
3	Likely	<60 percent	Approximately every 3-7 years
2	Not likely	<30 percent	Approximately every 7-10 years
1	Slight	<10 percent	Every 10 years and beyond or rarely

Internal Control Effectiveness



Score	Rating	Description
5	Effective	Controls are properly designed and operating as intended. Management activities are effective in managing and mitigating risks
4	Limited improvement needed	Controls and/or management activities are properly designed and operating somewhat effectively, with some opportunities for improvement identified
3	Significant improvement needed	Key controls and/or management activities in place, with significant opportunities for improvement identified
2	Ineffective	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
1	Highly ineffective	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

IV.3 Event Identification and Risk Assessment

Event Identification

Potential events shall be identified by collecting information from relevant management and other staff members within the organizational unit that is conducting the risk assessment, through individual interviews, workshops, risk questionnaires, and surveys. Risks may be as well identified from other sources, including process flow analyses, audit reports, incident reports, and past experience.

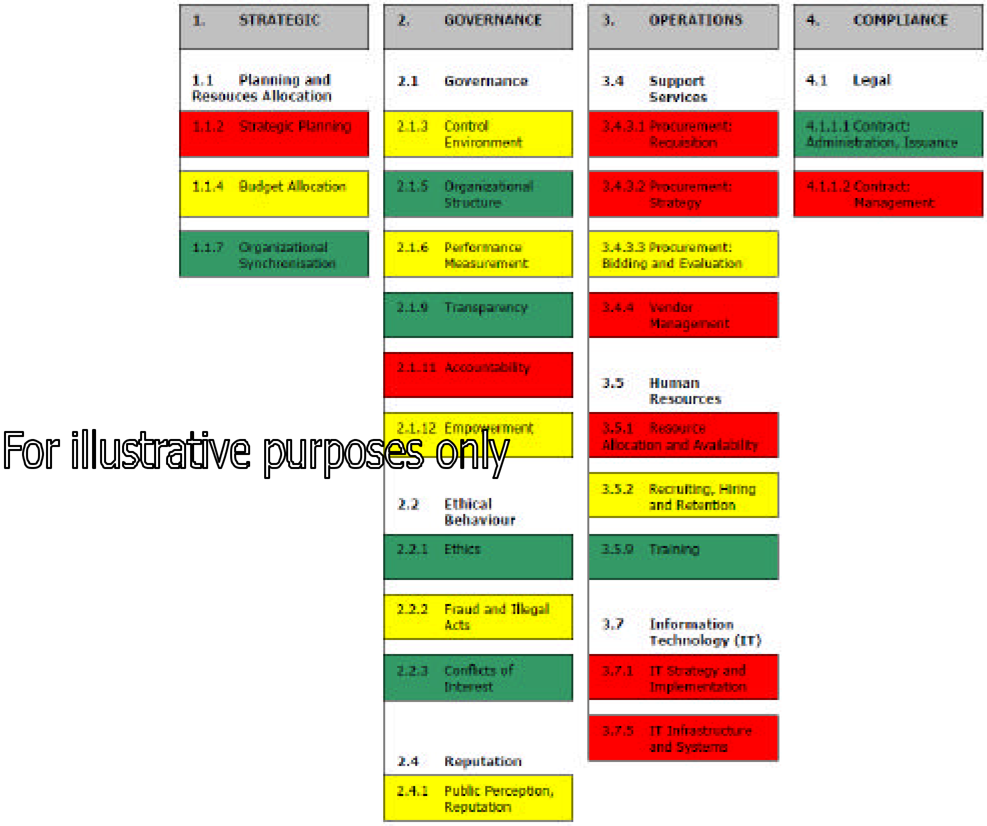
Performing the Risk Assessment

Each of the identified risks shall be then evaluated according to the previously 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, without the consideration of any existing internal controls established to mitigate the risk (*inherent risk* rating).

Appropriate input shall then be obtained to assess the effectiveness of internal controls or processes in place to mitigate the risk. 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.

The proper consideration of inherent risk exposure on one side, and the level of internal control effectiveness on the other, determines the level of *residual risk*. According to best practices, 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. These results shall be ultimately validated in a dedicated workshop so that management could share a common understanding of the identified risks and their criticality.

Figure 4 – Example of a Local Risk Universe


1. STRATEGIC
1.1 Planning and Resouces Allocation
1.1.2 Strategic Planning
1.1.4 Budget Allocation
1.1.7 Organizational Synchronisation
2. GOVERNANCE
2.1 Governance
2.1.3 Control Environment
2.1.5 Organizational Structure
2.1.6 Performance Measurement
2.1.9 Transparency
2.1.11 Accountability
2.1.12 Empowerment
2.2 Ethical Behaviour
2.2.1 Ethics
2.2.2 Fraud and Illegal Acts
2.2.3 Conflicts of Interest
2.4 Reputation
2.4.1 Public Perception, Reputation
3. OPERATIONS
3.4 Support Services
3.4.3.1 Procurement: Requisition
3.4.3.2 Procurement: Strategy
3.4.3.3 Procurement: Bidding and Evaluation
3.4.4 Vendor Management
3.5 Human Resources
3.5.1 Resource Allocation and Availability
3.5.2 Recruiting, Hiring and Retention
3.5.9 Training
3.7 Information Technology (IT)
3.7.1 IT Strategy and Implementation
3.7.5 IT Infrastructure and Systems
4. COMPLIANCE
4.1 Legal
4.1.1.1 Contract: Administration, Issuance
4.1.1.2 Contract: Management
For illustrative purposes only

Note: The above Local Risk Universe is a representation of a potential outcome from a programme Risk Assessment and is provided for illustration purposes only.

IV.4 Risk Response and Internal Control Activities

Analysis of Results

The ratings for impact, likelihood and internal control effectiveness resulting from the assessment of the identified risks, based on defined formulas, will then determine for each risk the overall *inherent risk exposure*[2], and following the proper consideration of the internal control measures, the *residual risk exposure*[3]. The resulting risks shall subsequently be classified into three tiers, based on the evaluation of both inherent and residual risk, and judgement based on contributing factors and the information gathered during the risk assessment process.

The most significant risks, categorised as Tier 1 risks, will require an adequate level of attention, and as such will be reported to the Management Committee, to the Secretary-General, and through the Secretary-General to the IAAC and the General Assembly.

Moderate risks (Tier 2) will typically require specific remedial or monitoring measures under the responsibility of the Risk Owner and the local Risk and Internal Control Focal Point. These risks shall be reported to the Enterprise Risk Management and Internal Control function and the Under-Secretary-General, or equivalent, responsible for the area under assessment.

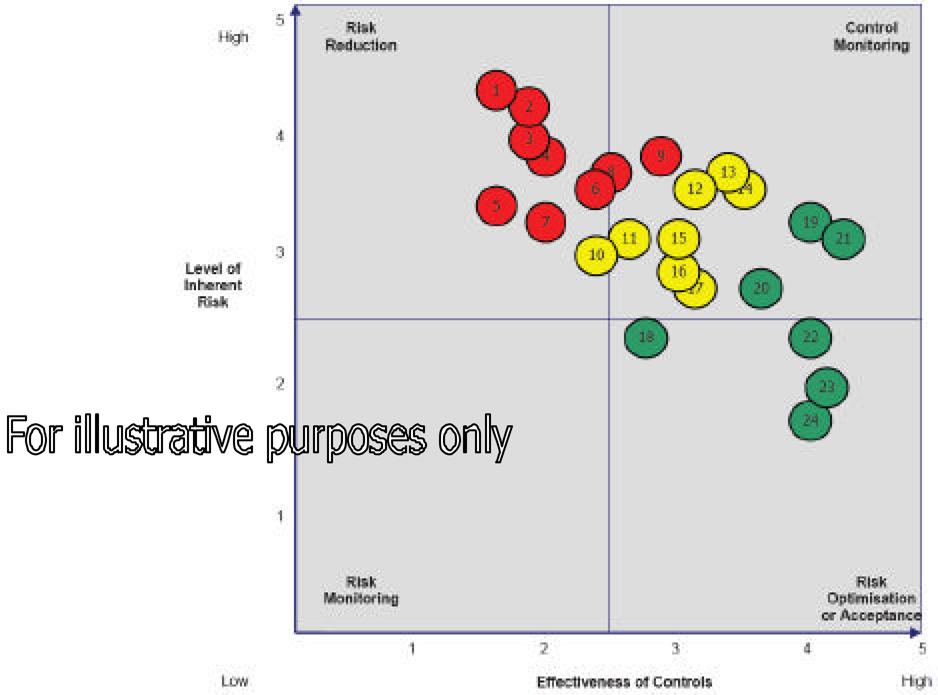
The risks expected to have a relatively low risk exposure and residual risk, will be classified as Tier 3 risks. Proper assurance on the stability of the risk level shall be provided through periodic monitoring. Some flexibility in risk treatment and budget allocation may be applicable to low risks, as management may decide to implement specific efficiency measures.

The Residual Risk Heat Map, a four-quadrant chart as depicted in Figure 5 below, will 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.

[2] Determined by taking the square root of impact multiplied by likelihood.

[3] Determined by subtracting the internal control effectiveness rating from the inherent risk exposure.

Figure 5 – Example of a Residual Risk Heat Map



Tier 1 Risks (Significant)	Tier 2 Risks (Moderate)	Tier 3 Risks (Lower)
1. IT Strategy and System Implementation (3.7.1) 2. IT Infrastructure and Systems (3.7.5) 3. Procurement: Requisition (3.4.3.1) 4. Contract Management(4.1.1.2) 5. Accountability (2.1.11) 6. Procurement: Strategy (3.4.3.2) 7. Vendor Management (3.4.4) 8. Resource Allocation and Availability (3.5.1) 9. Strategic Planning (1.1.2)	10. Empowerment (2.1.12) 11. Control Environment (2.1.3) 12. Fraud and Illegal Acts (2.2.2) 13. Procurement: Bidding and Bid Evaluation (3.4.3.3) 14. Public Perception (2.4.1) 15. Recruiting, Hiring and Retention (3.5.2) 16. Performance Measurement (2.1.6) 17. Budget Allocation (1.1.4)	18. Organizational Structure (2.1.5) 19. Conflicts of Interest (2.2.3) 20. Training (3.5.9) 21. Ethics (2.2.1) 22. Transparency (2.1.9) 23. Contract: Administration and Issuance (4.1.1.1) 24. Organizational Synchronisation (1.1.7)

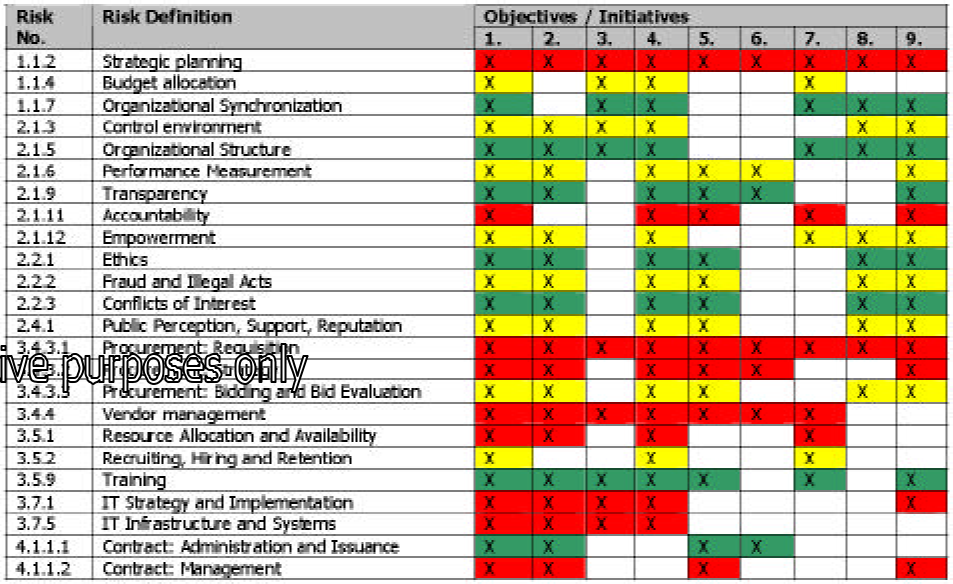
Note: The above Residual Risk Map is a representation of a potential outcome from a programme Risk Assessment and is provided for illustration purposes only.

Alignment of risks with Mandates, Objectives and Strategic Plans

Strategic plans are identified to support the mandates and objectives of the specific Department, Office, Commission, Mission, or Tribunal, as defined by the General Assembly. Enterprise risk management will take a process view towards risk, in which risk management is driven by organizational strategies and objectives, and the processes and initiatives that exists to achieve those strategies and objectives. The ability to appropriately link risks to both strategies and objectives and the underlying processes and activities is critical to the identification and implementation of effective risk mitigation measures.

The risk assessment, through the alignment of risks with objectives and plans, effectively facilitates the relationship between the risk management process and the budget process. 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



Risk No.	Risk Definition	Objectives / Initiatives								
		1.	2.	3.	4.	5.	6.	7.	8.	9.
1.1.2	Strategic planning	X	X	X	X	X	X	X	X	X
1.1.4	Budget allocation	X		X	X			X		
1.1.7	Organizational Synchronization	X		X	X			X	X	X
2.1.3	Control environment	X	X	X	X				X	X
2.1.5	Organizational Structure	X	X	X	X			X	X	X
2.1.6	Performance Measurement	X	X		X	X	X			X
2.1.9	Transparency	X	X		X	X	X			X
2.1.11	Accountability	X			X	X		X		X
2.1.12	Empowerment	X	X		X			X	X	X
2.2.1	Ethics	X	X		X	X			X	X
2.2.2	Fraud and Illegal Acts	X	X		X	X			X	X
2.2.3	Conflicts of Interest	X	X		X	X			X	X
2.4.1	Public Perception, Support, Reputation	X	X		X	X			X	X
3.4.3.1	Procurement: Requisition	X	X	X	X	X	X	X	X	X
[illegible]	[illegible]	X	X		X	X	X			X
3.4.3.3	Procurement: Bidding and Bid Evaluation	X	X		X	X			X	X
3.4.4	Vendor management	X	X	X	X	X	X	X		
3.5.1	Resource Allocation and Availability	X	X		X			X		
3.5.2	Recruiting, Hiring and Retention	X			X			X		
3.5.9	Training	X	X	X	X	X		X		X
3.7.1	IT Strategy and Implementation	X	X	X	X					X
3.7.5	IT Infrastructure and Systems	X	X	X	X					
4.1.1.1	Contract: Administration and Issuance	X	X			X	X			
4.1.1.2	Contract: Management	X	X			X				X

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

Determination of Risk Responses

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

(i) **Risk Reduction** – Risks characterised by a high inherent risk exposure and ineffective internal controls will fall in the "risk reduction" quadrant. A reduction in risk exposure could be achieved through different strategies, 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 inherent risk exposure and low internal control effectiveness will be included in this category. As even if these risks were to materialise, the impact upon 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 and Internal Control Focal Point, 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 and Internal Control 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, 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 risks 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 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, and identifying risk treatment owners, as illustrated by Figure 8 below.

Entity level risk assessment results

The results of the different risk assessments shall be collected by the Enterprise Risk Management and Internal Control function and compared within and across unit locations. As all risks and criteria shall ultimately be able to be traced back to those established at the entity level, risk results may be compiled and aggregated at the Organization level. The assessment outputs from the unit locations shall be compared by the Enterprise Risk Management and Internal Control function and measured against the entity level scoring criteria to provide an entity level risk assessment result. 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 budget preparation and evaluation process.

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 strategic framework and budgeting process. An effective enterprise risk management and internal control process will in this manner 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.

IV.5 Information and Communication

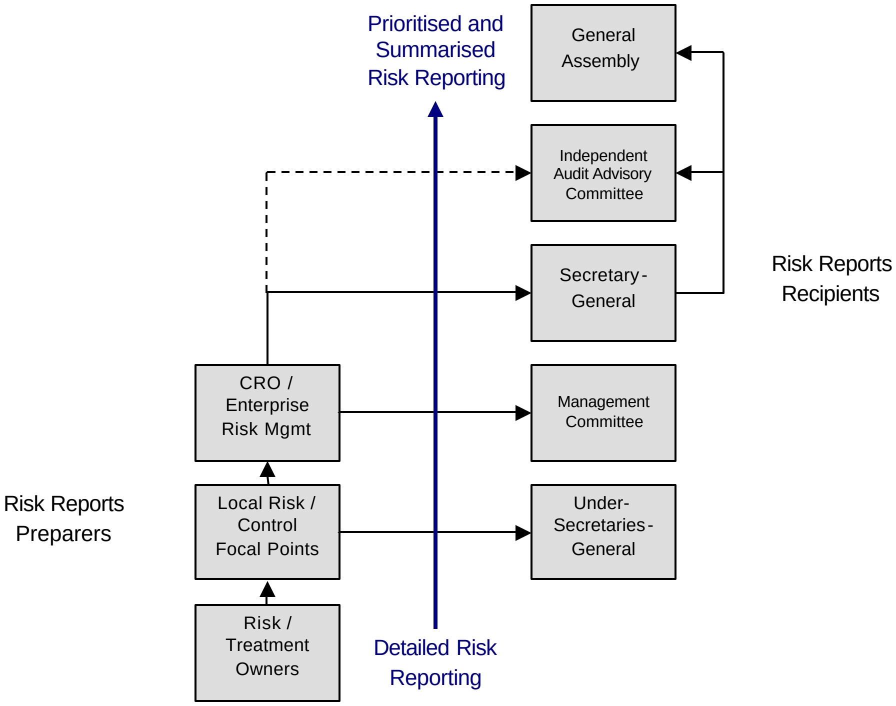
Relevant risk and internal control information shall be provided at the appropriate levels within the Organization, to adequately support decision making towards the achievement of established mandates and objectives.

The risks to be reported on, the level of details required, 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 entity-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 at the local level.

Risk reporting and its frequency are the primary mechanisms that provide relevant information on risk exposure to different levels within the Organization. The frequency of risk reporting shall as well depend upon the report recipients. Annual reporting shall be established to the General Assembly, through the ACABQ and IAAC, semi-annual reporting shall be defined for the Secretary-General and the Management Committee, whilst Under-Secretaries-General or equivalent position, the Enterprise Risk Management and Internal Control function, and local Risk and Internal Control Focal Points shall receive quarterly reports.

Figure 7 below provides a visual representation of the described risk reporting process:

Figure 7 – Risk reporting process


Prioritised and Summarised Risk Reporting
General Assembly
Independent Audit Advisory Committee
Secretary-General
Risk Reports Recipients
CRO / Enterprise Risk Mgmt
Management Committee
Risk Reports Preparers
Local Risk / Control Focal Points
Under-Secretaries-General
Risk / Treatment Owners
Detailed Risk Reporting

Risk Reports

According to best practice, the periodic risk reports that shall be prepared in support of risk management and internal control activities may include the documents described below. As mentioned, risk and internal control reporting shall be provided through the reporting and submission phases of the budget preparation and evaluation process, where applicable.

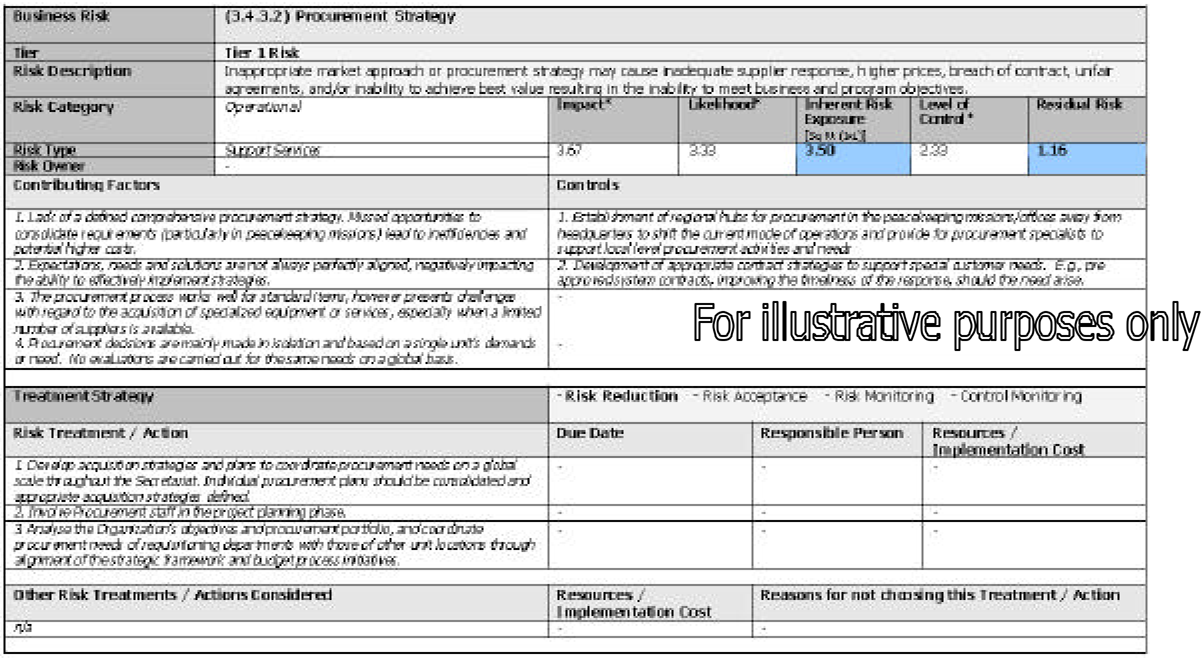
(i) **Risk Dashboard** – A graphical representation will provide a summary of the significant risks identified as a result of the risk assessment process, and shall be prepared both at the local level (Department, Office, Commission, Mission and Tribunal) and at the entity level on a consolidated basis, reflecting the combined output of the Organization, the risk description, and the factors that contribute to the risk, completed by an overview of the status of the treatment strategy. This report shall be distributed annually to the Management Committee and the Secretary-General and through the Secretary-General to the General Assembly through the ACABQ, and the IAAC.

(ii) **UN Secretariat Risk Report** – The risk report at entity level will include a representation of the results of the risk assessment on a "Residual Risk Heat Map", and incorporate additional details on the consolidated risks identified for the Organization, in particular on the risk contributing factors supporting the risk assessment, and the resulting action plans and proposed treatments. The risk report shall be prepared by the Enterprise Risk Management and Internal Control function, and distributed to the Management Committee and the Secretary-General semi-annually, or as required.

(iii) **Local Risk Report** (at the Department, Office, Commission, Mission or Tribunal level) – This report shall as well include the results of the risk assessment plotted on a “Residual Risk Heat Map”, identifying the risk contributing factors supporting the risk assessment, and resulting action plans and proposed treatments. This report will be distributed to senior management (Under-Secretary-General or equivalent) and the Enterprise Risk Management and Internal Control function quarterly, or as required.

(iv) **Risk Treatment and Response Plan** – Following the completion of the risk assessment, a comprehensive Risk Treatment and Response Plan shall be prepared by the responsible management in cooperation with the local Risk and Internal Control Focal Point and submitted to the Under-Secretary-General responsible for the Department or equivalent, and the Enterprise Risk Management and Internal Control function. Periodic status reports shall be prepared until the agreed risk mitigation measures have been fully implemented.

Figure 8 – Example of a Risk Treatment and Response Plan



Business Risk	**(3.4.3.2) Procurement Strategy**					
Tier	**Tier 1 Risk**					
Risk Description	Inappropriate market approach or procurement strategy may cause inadequate supplier response, higher prices, breach of contract, unfair agreements, and/or inability to achieve best value resulting in the inability to meet business and program objectives.					
Risk Category	*Operational*	**Impact***	**Likelihood***	**Inherent Risk Exposure** [Sq. M. (IxL)]	**Level of Control ***	**Residual Risk**
Risk Type	Support Services	3.67	3.33	**3.50**	2.33	**1.16**
Risk Owner	-					

Contributing Factors	**Controls**
1. Lack of a defined comprehensive procurement strategy. Missed opportunities to consolidate requirements (particularly in peacekeeping missions) lead to inefficiencies and potential higher costs.	*1. Establishment of regional hubs for procurement in the peacekeeping missions/offices away from headquarters to shift the current mode of operations and provide for procurement specialists to support local level procurement activities and needs*
2. Expectations, needs and solutions are not always perfectly aligned, negatively impacting the ability to effectively implement strategies.	*2. Development of appropriate contract strategies to support special customer needs. E.g, pre approved system contracts, improving the timeliness of the response, should the need arise.*
3. The procurement process works well for standard items, however presents challenges with regard to the acquisition of specialized equipment or services, especially when a limited number of suppliers is available.	-
4. Procurement decisions are mainly made in isolation and based on a single unit's demands or need. No evaluations are carried out for the same needs on a global basis.	-

Treatment Strategy	- **Risk Reduction** - Risk Acceptance - Risk Monitoring - Control Monitoring		
Risk Treatment / Action	**Due Date**	**Responsible Person**	**Resources / Implementation Cost**
1. Develop acquisition strategies and plans to coordinate procurement needs on a global scale throughout the Secretariat. Individual procurement plans should be consolidated and appropriate acquisition strategies defined.	-	-	-
2. Involve Procurement staff in the project planning phase.	-	-	-
3. Analyse the Organization's objectives and procurement portfolio, and coordinate procurement needs of requisitioning departments with those of other unit locations through alignment of the strategic framework and budget process initiatives.	-	-	-

Other Risk Treatments / Actions Considered	**Resources / Implementation Cost**	**Reasons for not choosing this Treatment / Action**
n/a	-	-

Note: The above Risk Treatment and Response Plan is a representation of a potential outcome from a programme Risk Assessment and is provided for illustration purposes only.

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 with regard to the effectiveness of designed controls and the appropriateness of defined risk treatments. The local Risk and Internal Control Focal Points and the Enterprise Risk Management and Internal Control function shall assist management with ongoing monitoring and reporting as to the effectiveness of risk management and internal control activities.

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 with regard to 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 will require the capability to automate many of the activities, tools, and reports critical to the programme's successful implementation. The automation of the framework will provide for 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.

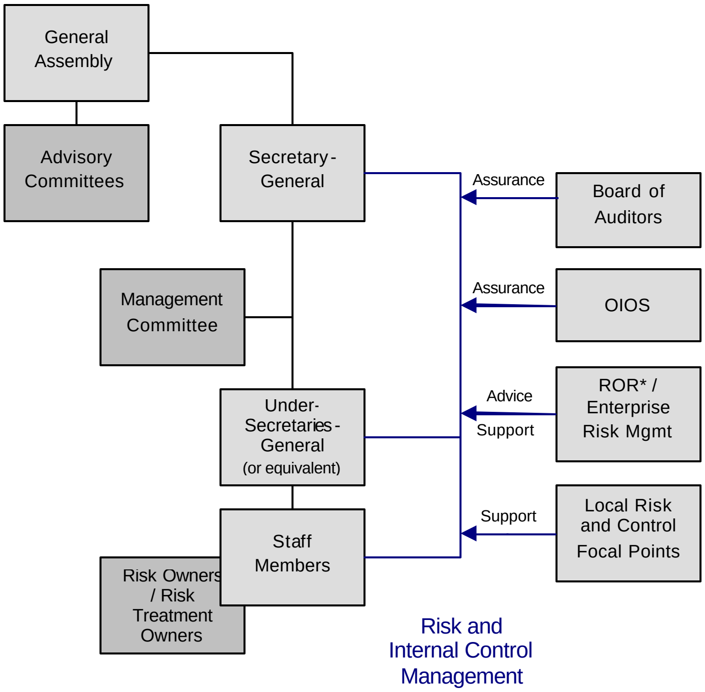
The ERM system shall be designed to incorporate the various and diverse elements of the framework, including a linked database repository of risks and risk information (the risk register), and the capability to support and measure risk on an inherent and a residual basis at a variety of different levels 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.

V. Risk Governance, Roles and Responsibilities

Risk Governance

Proper risk governance mechanisms are critical for the adoption of an effective risk management framework. Figure 9 below provides an overview of the governance structure as outlined by this framework, and is followed by a description of the roles and responsibilities of the different functions involved.

Figure 9 – Risk governance structure


General Assembly
Advisory Committees
Secretary-General
Management Committee
Under-Secretaries-General (or equivalent)
Staff Members
Risk Owners / Risk Treatment Owners
Assurance
Board of Auditors
Assurance
OIOS
Advice
Support
ROR* / Enterprise Risk Mgmt
Support
Local Risk and Control Focal Points
Risk and Internal Control Management

*High level official responsible for risk within the Organization

General Assembly

The General Assembly, with the advice of the Advisory Committee on Administrative and Budgetary Questions and the Independent Audit Advisory Committee, provides risk management oversight, 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. The Secretary-General annually reviews with the Management Committee the significant risks faced by the Organization, and the proposed strategies designed to effectively mitigate the identified risks at a consolidated entity level, and accordingly reports to the General Assembly and the IAAC.

Management Committee

The Management Committee, acting as Enterprise Risk Management Committee for the Secretariat, annually reviews the results of the risk assessments, and has an active role in the promotion of the best practices in risk and internal control management in the Organization, involving as well the Policy Committee on relevant policy matters, as may be appropriate. The Management Committee shall as well monitor the effectiveness of the enterprise risk management and internal control framework and recommend any changes that may be required.

Under-Secretaries-General (or equivalent positions)

At the level of each Department, Office, Commission, Mission, or Tribunal, responsibility for the effective implementation risk management and internal control practices, as described by this framework, resides with the respective Head of Department, Office, Commission, Mission, or Tribunal.

As part of the existing senior management compacts with the Secretary-General, each Under-Secretary-General (or equivalent position) shall annually confirm through a *Certification Report* 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 mission and objectives of the area of responsibility in the definition of the relevant risks and strategies, and implementing a risk management process following the guidelines of the approved framework.

(ii) Ensuring that risks are appropriately 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 to 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 elevating significant and emerging risks to the Management Committee, and the Secretary-General.

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

Local Risk and Internal Control Focal Points

As previously described, local Risk and Internal Control Focal Points shall be part of each Department, Office, Commission, Mission and Tribunal, with solid reporting lines to local management, and dotted reporting lines to the Enterprise Risk Management and Internal Control function, to support the implementation of risk assessment and risk and internal control monitoring activities, as further described below. Responsibilities shall be assigned to one or more existing staff, on a part-time basis, or as deemed suitable by the responsible management considering the complexities of the underlying operations. Local Risk and Internal Control Focal Points shall be nominated for each Department, Office, Commission, Mission and Tribunal. In particular:

Offices Away from Headquarters

(i) Economic and Social Commission for Asia and the Pacific ("ESCAP")

(ii) Economic and Social Commission for Western Asia ("ESCWA")

(iii) Economic Commission for Africa ("ECA")

(iv) Economic Commission for Europe ("ECE")

(v) Economic Commission for Latin America and the Caribbean ("ECLAC")

(vi) International Criminal Tribunal for Rwanda ("ICTR")

(vii) International Criminal Tribunal for the Former Yugoslavia ("ICTY")

(viii) Office of the High Commissioner for Human Rights ("OHCHR")

(ix) Office of the High Commissioner for Refugees ("UNHCR")

(x) Office on Drugs and Crime ("UNODC")

(xi) United Nations Conference on Trade and Development ("UNCTAD")

(xii) United Nations Environment Programme ("UNEP")

(xiii) United Nations Human Settlement Programme ("UN-HABITAT")

(xiv) United Nations Office at Geneva ("UNOG")

(xv) United Nations Office at Nairobi ("UNON")

(xvi) United Nations Office at Vienna ("UNOV")

(xvii) United Nations Relief and Works Agency for Palestine Refugees in the Near East ("UNRWA")

(xviii) United Nations University ("UNU")

Headquarters (New York)

(i) Office of the Secretary-General ("OSG")

(ii) Counter-Terrorism Committee Executive Directorate ("CTED")

(iii) Department for General Assembly and Conference Management ("DGACM")

(iv) Department of Economic and Social Affairs ("DESA")

(v) Department of Field Support ("DFS")

(vi) Department of Management ("DM")

(vii) Department of Peace Keeping Operations ("DPKO")

(viii) Department of Political Affairs ("DPA")

(ix) Department of Public Information ("DPI")

(x) Department of Safety and Security ("DSS")

(xi) Office for Disarmament Affairs ("UNODA")

(xii) Office for the Coordination of Humanitarian Affairs ("OCHA")

(xiii) Office of High Representative for the Least Developed Countries, Landlocked Developing Countries and Small Island Developing States ("UN – OHRLLS")

(xiv) Office of Internal Oversight Services ("OIOS")

(xv) Office of Legal Affairs ("OLA")

(xvi) Office of the Special Adviser on Africa ("OSAA")

(xvii) Office of the Special Representative of the Secretary General for Children and Armed Conflict ("OSRSG-CAC")

The responsibilities of local Risk and Internal Control 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, objectives and mandates at the Department, Office, Commission, Mission or Tribunal level; the completion of the risk assessment and reporting on its results; the proposal of the activities that should included in the Risk Treatment and Response Plan; and the provision of 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 reflects the risks relevant to the Department, Office, Commission, Mission or Tribunal; prepare reports on all risk management matters, and distribute them to the Enterprise Risk Management and Internal Control function, and the responsible Under-Secretary-General, or equivalent position; and monitor the effectiveness of risk management and internal control measures.

Risk Owners

Risk owners are responsible, amongst other matters, for:

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

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

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

Risk Treatment Owners

The design and implementation of risk treatment and response plans identified during the risk assessment process is the responsibility of risk treatment owners. Their responsibilities involve implementing the risk treatments for which they are responsible, and reviewing their effectiveness.

Enterprise Risk Management and Internal Control function

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

An Enterprise Risk Management and Internal Control function, that for the short term shall be established in the Office of the Under-Secretary-General for Management, shall assist senior management in the process of establishment of the described framework, and provide the appropriate level of implementation and execution oversight. According to the best practice in both private and public sector global organizations that have adopted enterprise-wide risk management frameworks, the Enterprise Risk Management and Internal Control function shall progressively move towards a future state design stage of separate management function led by a senior management official reporting to the highest level of the Organization and the Management Committee, once the function is supported by adequate resources and appropriate processes are established, in order to ensure the effectiveness of the risk management process.

Without establishing a new high-level full-time responsible official for risk in the Organization, a senior management official, acting in this capacity, shall coordinate all the activities of the Enterprise Risk Management and Internal Control function. He or she will act independently and objectively in the execution of his/her duties and responsibilities, fully in line with the JIU recommended benchmarks[4].

As management shall be the owner of risk management and internal control activities, the Enterprise Risk Management and Internal Control function shall have among its main responsibilities the overall facilitation of the effective implementation of the enterprise risk management and internal control framework process, providing assistance to the different Offices, Departments, Missions, Commissions and Tribunals in implementing risk management and internal control procedures based on systematic risk mitigation strategies consistently applied across the Organization, aggregating risk data from the different unit locations, and carrying out regular monitoring of UN Secretariat-wide risks.

The Enterprise Risk Management and Internal Control function 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 Department, Office, Commission, Mission and Tribunal level, cooperating with dedicated Risk and Internal Control 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 Enterprise Risk Management and Internal Control function include:

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

[4] Paragraph 91 and 94, JIU/REP/2010/4.

(ii) Defining a comprehensive enterprise risk management and internal control 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 Risk Register, and facilitating the performance of the risk assessment through assistance in interviews, development and review of questionnaires, and facilitation of 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.

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

(vi) Preparing reports on risk management and internal control activities, including a consolidated entity level risk assessment report for the UN Secretariat, 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 and internal control activities at the Department, Office, Commission, Mission and Tribunal level, and advising as appropriate on the development of adequate Risk Treatment and Response Plans.

(viii) Implementing and maintaining the necessary systems and data management capabilities to properly support the risk management and internal control programme.

(ix) Supporting the dissemination of information and best practices with regard to risk and internal control management principles and measures across the Organization, and developing as appropriate communication and training programs, to enhance the Secretariat's risk management culture.

(x) Assessing the risk of not implementing non-accepted recommendations and advising the Management Committee on possible courses of action.

Management and Staff Members

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

(i) Embedding risk management in 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 accordingly 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 and Internal Control Focal Points, and the Enterprise Risk Management and Internal Control function, when due.

(v) Providing visible support to the implementation of the Secretariat's enterprise risk management and internal control 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 enterprise risk management and internal control 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

Annex 1.

United Nations Secretariat Risk Universe

1. STRATEGIC

1.1 Planning and resource allocation

1.1.1 Vision and mandate

1.1.2 Strategic planning

1.1.3 Budgeting

1.1.4 Budget allocation

1.1.5 Human resources strategy and planning

1.1.6 Planning execution and integration

1.1.7 Organizational synchronization

1.1.8 Overlapping mandates

1.1.9 Outsourcing

1.2 Principal organs, members and partners

1.2.1 General Assembly and Member States

1.2.2 Partners, affiliates, agencies and donors

1.2.3 Organizational relationships

1.3 Internal and external factors

1.3.1 Political climate — external

1.3.2 Political climate — internal

1.3.3 Economic factors — commodity prices

1.3.4 Unique events (i.e., pandemic, election, environmental crisis)

1.3.5 Organizational transformation

2. GOVERNANCE

2.1 Governance

2.1.1 Tone at the top

2.1.2 Secretariat, councils and committees

2.1.3 Control environment

2.1.4 Decision-making — General Assembly, Security Council and committees

2.1.5 Organizational structure

2.1.6 Performance measurement

2.1.7 Performance management

2.1.8 Joint inter-agency operation and partnering

2.1.9 Transparency

2.1.10 Leadership and management

2.1.11 Accountability

2.1.12 Empowerment

2.2 Ethical behaviour

2.2.1 Ethics

2.2.2 Fraud and illegal acts

2.2.3 Conflicts of interest

2.2.4 Professional conduct and confidentiality

2.3 Communications and public relations

2.3.1 Media relations and public information

2.3.2 Crisis communications

2.3.3 Personnel communications

2.3.4 Broadcast — radio and television

2.3.5 Technology communication

2.4 Reputation

2.4.1 Public perception, support and reputation

2.4.2 Crisis and contingency planning and management

3. OPERATIONS

3.1 Programme management

3.1.1 Advocacy

3.1.2 Outreach activities

3.1.3 Economic and social development

3.1.4 Conference management

3.1.5 Research, analysis and advisory activities

3.1.6 Policy development

3.1.7 Inter-agency cooperation and liaison activities

3.2 Mission activities

3.2.1 International peace and security

3.2.2 Electoral support

3.2.3 Rule of law

3.2.4 Disaster response and humanitarian assistance

3.2.5 Mission planning

3.2.6 Mission start-up

3.2.7 Mission liquidation

3.2.8 Logistics

3.2.9 Air, land and sea operations

3.2.10 Engineering

3.2.11 Communications

3.2.12 Mission staffing

3.2.13 Mission creep

3.3 International tribunals

3.3.1 Investigations and prosecution

3.3.2 Trials and appeals

3.3.3 Witness protection

3.3.4 Completion strategy

3.3.5 Residual capacity and activities

3. OPERATIONS (continued)

3.4 Support services

3.4.1 Funding

3.4.2 Translation and interpretation

3.4.3 Procurement

3.4.4 Supplier management

3.4.5 Asset and inventory management

3.4.6 Facilities and real estate management

3.4.7 Capital master planning

3.4.8 Business continuity

3.4.9 Commercial activities

3.4.10 Legal aid

3.4.11 Court management and legal support

3.4.12 Detention unit management

3.5 Human resources

3.5.1 Resource allocation and availability

3.5.2 Recruiting, hiring and retention

3.5.3 Succession planning and promotion

3.5.4 Conduct and discipline

3.5.5 Development and performance

3.5.6 Compensation and benefits

3.5.7 Medical services

3.5.8 Safety and security

3.5.9 Training

3.5.10 Mobility

3.6 Intellectual property

3.6.1 Knowledge management

3.6.2 Information and document management

3.7 Information resources and information technology

3.7.1 IT strategy and system implementation

3.7.2 IT security and access

3.7.3 IT availability and continuity

3.7.4 IT integrity

3.7.5 IT infrastructure and systems

4. COMPLIANCE

4.1 Legal

4.1.1 Contract

4.1.2 Intellectual property

4.1.3 Anti-corruption

4.1.4 International law

4.1.5 Privacy

4.2 Regulatory

4.2.1 Internal policies and resolutions

4.2.2 United Nations labour relations

4.2.3 Host country regulations

5. FINANCIAL

5.1 Funding and investments

5.1.1 Financial contributions

5.1.2 Extrabudgetary funding

5.1.3 Trust funds — receipt of cash

5.1.4 Trust fund management

5.1.5 Donor fund management and reporting

5.1.6 Cash management

5.1.7 Investments

5.1.8 Financial markets

5.1.9 Insurance

5.2 Accounting and reporting

5.2.1 Financial management and reporting

5.2.2 General accounting

5.2.3 Financial controls

5.2.4 Liability management and disbursements

5.2.5 Staff tax reimbursements

Annex 2.

Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control Effectiveness

Impact

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

Scoring criteria for the measurement of Impact, Likelihood and Level of Internal Control Effectiveness

Likelihood

Score	Rating	Certainty	Frequency
5	Expected	>90 percent	At least yearly and/or multiple occurrences within the year
4	Highly likely	<90 per cent	Approximately every 1-3 years
3	Likely	<60 per cent	Approximately every 3-7 years
2	Not likely	<30 per cent	Approximately every 7-10 years
1	Slight	<10 per cent	Every 10 years and beyond or rarely

Level of Internal Control / Management Effectiveness

Score	Rrating	Description
5	Effective	Controls are properly designed and operating as intended. Management activities are effective in managing and mitigating risks
4	Limited improvement needed	Controls and/or management activities are properly designed and operating somewhat effectively, with some opportunities for improvement identified
3	Significant improvement needed	Key controls and/or management activities in place, with significant opportunities for improvement identified
2	Ineffective	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
1	Highly ineffective	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

Annex 3.

Glossary of Terms and Definitions[5]

Term	***Definition***
Enterprise Risk Management	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.
Inherent Risk	The risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact.
Internal Control	A process, effected by governing bodies, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (i) Effectiveness and efficiency of operations; (ii) Reliability of financial reporting; (iii) Compliance with applicable laws and regulations.
Impact	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.
Likelihood	The possibility that a given event will occur.
Reasonable assurance	The concept that enterprise risk management, even if well designed and operated, can not 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.

[5] Consistent with the best international standards, as "Enterprise Risk Management - Integrated Framework" and "Thought Papers on Enterprise Risk Management", Committee of Sponsoring Organizations of the Treadway Commission, 2004, 2009, 2010 and 2011;
"Guidelines for Internal Control Standards for the Public Sector", Internal Control Standards Committee of the International Organization of Supreme Audit Institutions, 2004 and 2007; and
"Risk management – Principles and Guidelines" – International Organization for Standardization, 2009.

Term	***Definition***
Residual Risk	The remaining risk after management has taken action to alter the risk's likelihood or impact.
Residual Risk Heat Map	Inherent Risk 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 (Impact times Likelihood) and Level of Risk Mitigation Activities or Internal Control Effectiveness.
Risk	The effect of uncertainty on objectives.
Risk Appetite	The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission.
Risk Dashboard	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 critical to the Organization.
Risk Exposure	Magnitude of a risk measured in terms of the combination of Impact and Likelihood.
Risk Register	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.
Risk Tolerance	The acceptable variation relative to the achievement of an objective.
Risk Universe, or Risk Catalogue	Extract of the Risk Register containing the risk category, sub-category, risk and risk definition.
Tier 1 Risks	Significant 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.
Tier 2 Risks	Moderate Risks – Those risks which may require focus and some remedial or monitoring action.
Tier 3 Risks	Lower Risks – Those risks determined to have a relatively low exposure and residual risk and that require periodic monitoring to provide assurance that the level of risk remains constant.

Annex 4.

United Nations Secretariat Risk Catalogue: Risk Definitions

Risk Category		**Risk Definition**
Risk		
1. STRATEGIC – Relating to high-level goals, aligned with and supporting the Organization’s charter, vision and mandate		
1.1	**Planning and Resource Allocation**	
1.1.1	Vision and Mandate	Failure to establish a clear vision and direction for major Secretariat-wide initiatives to support the achievement of Secretariat mandates and objectives. Failure to establish clear programme criteria and adequately measure progress against the criteria.
1.1.2	Strategic Planning	Inability to discover, evaluate and select among alternatives to provide direction and allocate resources for effective execution in achieving the mission, mandate and objectives of the Secretariat and supporting Departments, Offices, and Commissions, creating a lack of clarity in decision-making and confusion within the oversight entities.
1.1.3	Budgeting	Inability to effectively budget or to fully spend approved funds for operations and activities critical to achievement of mandate, goals and objectives and corresponding initiatives of the Secretariat and supporting Departments, Offices, and Commissions. May also result in loss of confidence by Member States and others in ability to budget and forecast fiscal needs and requirements.
1.1.4	Budget Allocation	Budget requests are not completely fulfilled impeding ability to effectively carry out mission, objectives, duties, plans and strategies. Day to day operations or unanticipated surges in workload can be affected by insufficient resources to carry out planned objectives and mandates. Budgetary requirements may not be appropriately articulated or evaluated relative to perceived objectives or needs. Existence of a rigid budget structure which prevents redeployment of funds and encourages over-use.
1.1.5	HR Strategy and Planning	Failure to have a well-defined People and HR Strategy that supports the organizational and strategic objectives, employee needs and desired organizational mission, vision, and values.
1.1.6	Planning Execution and Integration	Failure to execute and integrate specific activities to initiate a change in strategic or operational direction, mandates or objectives.
1.1.7	Organizational Synchronization	Lack of synchronization of objectives and priorities and coordination between HQ, other offices and the field.
1.1.8	Overlapping Mandates	Lack of clear delineation of roles and responsibilities for thematic areas across the UN system, and ambiguity regarding the direction of the One-UN project, creates competition within the UN

Risk Category		**Risk Definition**
Risk		
		System that leads to confusion of the clients for the services, complicates inter-agency coordination and spreads resources thinly across the various agencies.
1.1.9	Outsourcing	Failure to optimize organizational efficiency and effectiveness through selecting appropriate outsourcing arrangements.
1.2	**Principal Organs, Members and Partners**	
1.2.1	General Assembly and Member States	Failure or inability to effectively monitor, assess, react to, and/ or meet the needs and expectations of the General Assembly or Member States. Contradictory or conflicting instructions and mandates and lack of clear consensus in decision making complicate the ability of the Secretariat to effectively execute and achieve planned strategies and objectives.
1.2.2	Partners, Affiliates, Agencies and Donors	Failure or inability to effectively monitor, assess, react to, and/ or meet the needs and expectations of affiliated entities, agencies, partners or donors. Perceived or actual conflicts of interest, resulting from “global compact” and dual role of certain supporting businesses as UN donors, partners and vendors.
1.2.3	Organizational Relationships	Confusing and/or ambiguous mandates, lack of consensus and / or changing, divergent or controversial stakeholder expectations restrain and/or negatively impact the UN's ability to act and hinders the timely and / or effective execution of important strategic and operational objectives and activities.
1.3	**Internal and External Factors**	
1.3.1	Political Climate – External	Adverse political events or prejudicial actions in a country or region, or failure of national governments to sustain their support for economic, humanitarian or peace-keeping efforts affect the Organization’s objectives and/or the capability to carry out its duties and missions.
1.3.2	Political Climate – Internal	Failure of Member States, the General Assembly or intergovernmental Committees to effectively address or respond to the needs of the UN Secretariat (funds, resources, etc.) to facilitate ability to meet objectives and mandates.
1.3.3	Economic Factors – Commodity Prices	Increasing costs of critical commodities such as food and medicine, adversely affect the level of outputs achievable by the Organization and the ability of the Organization to meet planned objectives.
1.3.4	Unique Events (i.e. pandemic, election, environmental crisis)	Inability to react timely with proper support and resources. Lack of appropriate resources to address situation or event.
1.3.5	Organizational Transformation	Inability of the Organization to respond to the needs of a changing environment. Conservative, risk-averse culture hinders the ability of the Organization to be flexible and responsive to change.

Risk Category		**Risk Definition**
	Risk	
2. GOVERNANCE – Related to organizational decisions or the implementation of those decisions		
2.1	**Governance**	
2.1.1	Tone at the Top	Failure of Secretariat leadership to set the appropriate tone, act with integrity and lead by example and/or to establish and maintain an infrastructure and environment that exemplifies an operating style of integrity, ethical values and competence of people. Unethical leadership behaviour negatively reflects on the Organization's ethics.
2.1.2	Secretariat, Councils and Committees	Failure of the General Assembly, Committees and / or Secretariat to discharge their respective obligations and duties in accordance with the UN Charter and mandates leads to loss of trust and support of Member States and others.
2.1.3	Control Environment	Failure to establish, maintain and reinforce an effective internal control environment which appropriately aligns and supports stakeholder expectations and organizational objectives and/or supports the UN's ability to operate efficiently and effectively in the achievement of its mission and mandate.
2.1.4	Decision Making – General Assembly, Security Council and Committees	Failure of the General Assembly, Security Council or other Committees to act timely or authoritatively.
2.1.5	Organizational Structure	The overall structure of the UN Organization does not support the achievement of strategic, mandated, operational and other organizational and operating objectives in an efficient and effective manner. Lack of clarity as to organizational structure and responsibilities and objectives of the UN Secretariat and other UN departments or agencies leads to confusion, conflicting or redundant activities, and ultimately, loss of public and Member State trust and confidence in the Secretariat's ability to achieve stated objectives.
2.1.6	Performance Measurement	Lack of defined performance measures and / or failure to define performance measurement criteria that is consistently applied and aligned with the core mission, mandate and objectives of the Secretariat and supporting Departments, Offices, and Commissions. Failure to effectively leverage and align performance measure outputs within or across Departments to improve planning, budgeting, forecasting, resource allocation and other activities critical to achieving the mission, mandate and objectives of the UN.
2.1.7	Performance Management	Failure to identify appropriate metrics and performance criteria, and assess performance quality and adherence to the standards and criteria as set forth by the Secretariat and General Assembly.
2.1.8	Joint Inter-agency Operations and Partnering Activities	Objectives of joint inter-agency operations and other partnering activities, and expectations of leadership are not appropriately aligned with one another or with the UN purpose, principles,

Risk Category		**Risk Definition**
Risk		
		mandates and objectives.
2.1.9	Transparency	Lack of transparency in decision making and communications fails to create trust or commitment and goodwill of Member States, staff and the general public.
2.1.10	Leadership and Management	The personnel responsible for managing and controlling an organization or a process do not possess the requisite knowledge, skills, experience, and/or managerial acumen needed to ensure that critical objectives are achieved and significant risks reduced to an acceptable level.
2.1.11	Accountability	Failure to promote accountability or otherwise hold responsible parties or constituents (UN Secretariat, agencies, Member States, staff and others) accountable for actions or inaction.
2.1.12	Empowerment	Lack of alignment between the authority given to employees commensurate with their responsibilities.
2.2	**Ethical Behaviour**	
2.2.1	Ethics	Absence of comprehensive formal ethical standards that are intended to direct and influence the way business or activities are conducted, above and beyond the letter of the law.
2.2.2	Fraud and Illegal Acts	Potential fraudulent illegal acts committed by staff, vendors and third parties expose the Organization to sanctions and loss of donors, resources and reputation. Financial loss due to unauthorized use or theft of the organization's physical, financial or information assets.
2.2.3	Conflicts of Interest	Acts committed by UN personnel, vendors and third parties for their personal benefit that ultimately impede the Organization's ability to sustain operations and operate effectively.
2.2.4	Professional Conduct and Confidentiality	Lack of awareness or acknowledgement of what constitutes professional conduct and confidential information or adherence to rules of professional conduct and requirements for maintaining confidentiality. Breach of rules of professional conduct and misuse of confidential information leads to loss of trust and confidence in Secretariat by the general public, Member States and staff.
2.3	**Communications and Public Relations**	
2.3.1	Media Relations and Public Information	Inability to anticipate and manage shifts in the information stakeholders want, and the way in which they want it communicated to them; and ineffective ongoing, transparent communications with the public in order to create goodwill.
2.3.2	Crisis Communications	Failure to effectively communicate or deliver the right message in times of crisis or disruption due to physical or natural circumstances or unique events.
2.3.3	Personnel Communications	Inability to understand, and respond to, the communication needs of different UN personnel (staff, volunteers, representatives, etc.).

Risk Category		**Risk Definition**
Risk		
2.3.4	Broadcast-radio and Television	Inability to broadcast the UN message to intended audience. Examples: - Inadequate infrastructure to reach the intended audience - Message not consistent or coherent with UN mission and mandate
2.3.5	Technology Communication	Misuse of Technology for Communication. The technology chosen to communicate internally and externally directly or indirectly contributes to, or fails to prevent, inflammatory, prejudicial or adverse situations or events resulting in material damage to the UN's image or reputation (e.g., mass emails, non-compliant emails, improper use of UN systems for communication, poor control over access to secure information / records, etc.).
2.4	**Reputation**	
2.4.1	Public Perception, Support and Reputation	The Organization may lose key personnel, contributors, and other partners or alliances and Member States' support due to negative publicity, reported illegal acts, inability to meet set operational objectives, and/or non-compliance with rules and regulations. Inability to appropriately react and respond to adverse publicity.
2.4.2	Crisis and Contingency Planning and Management	Failure to plan for, and effectively react to unanticipated and unique turn of events (both beneficial and adverse).
3. OPERATIONS – Relating to effective and efficient use of the Organization's resources		
3.1	**Programme Management**	
3.1.1	Advocacy	Failure to effectively advocate the causes that are integral to the mission and mandate of the specific Department/Office/Commission/Mission.
3.1.2	Outreach Activities	Ineffective or overlapping activities impede the ability of the Department, Office or Commission to effectively facilitate or provide the intended resolution or education or to support the activity's objective or mandate.
3.1.3	Economic and Social Development	Failure or inability to obtain or provide sufficient resources to support activities or to provide a framework for promoting and monitoring the implementation of plans, strategies and programmes in the economic and social fields.
3.1.4	Conference Management	Inability to service meetings. Failure to provide timely and accurate documentation to Member States, intergovernmental organs and expert bodies.
3.1.5	Research, Analysis and Advisory Activities	Inability to adequately analyse trends, compile and disseminate analytical data. Insufficient capabilities to effectively manage workflows or analyse underlying research data due to insufficient funding, human and / or technology tools and resources. Lack of access to necessary research information and data.

Risk Category		**Risk Definition**
Risk		
3.1.6	Policy Development	Inability to adequately support Member States' policy development needs. Inability to react to the demands for policy development. Contradictory positions among Member States render the policies inadequate or result in incoherent policies or policies that do not address the mandate.
3.1.7	Inter-agency Cooperation and Liaison Activities	Failure to effectively coordinate and align activities and requirements (including consensus as to controls and governance) with other agencies or programmes within the UN system.
3.2	**Mission Activities**	
3.2.1	International Peace and Security	Failure to respond timely and/or effectively can result in inability to achieve peace and security mission objectives and intended outcomes.
3.2.2	Electoral Support	Lack of support from the host country and/or insufficient resources affect the Organization's ability and capability to support the electoral process.
3.2.3	Rule of Law	Lack of support and/or infrastructure from the host country, insufficient or inadequately trained resources, and/or lack of integration between the local police force, and the judicial and correctional facilities affect the Organization's capability to strengthen the rule of law in accordance with its mandates.
3.2.4	Disaster Response and Humanitarian Assistance	Inability to react quickly or respond timely to natural or other disasters and/or requests for humanitarian aid or relief.
3.2.5	Mission Planning	Inability to discover, evaluate and select among appropriate alternatives to provide direction and effectively allocate resources (funding, staffing, equipment, supplies, etc.) to achieve mission objectives as defined.
3.2.6	Mission Start-up	Inability to develop a plan and schedule to meet start-up dates and/or start-up needs of a mission or programme and implement an appropriate plan or schedule sufficient to meet the immediate start-up needs and / or response time.
3.2.7	Mission Liquidation	Inability to develop a liquidation plan and schedule to meet anticipated wind-down and withdrawal dates and activities, including planned disposal, severance or redeployment of resources, equipment and staff.
3.2.8	Logistics	Inability to plan, coordinate, move and/or deploy the equipment, inventory, supplies, and human resources necessary to operate and support a mission and mission activities and objectives.
3.2.9	Air, Land and Sea Operations	Failure to provide for effective logistics capabilities in terms of ground transport and strategic air and sea lift for movement of military and civilian personnel and cargo. Failure or inability to appropriately schedule, manage, deploy, house or maintain resources and equipment.
3.2.10	Engineering	Failure to provide accommodation (office, living, warehouses, utilities and infrastructure) to the missions.
3.2.11	Communications	Failure to build the infrastructure necessary to effectively communicate among field operations

Risk Category		**Risk Definition**
Risk		
		and mission headquarters/regional offices may prevent the mission from achieving its mandate. Failure to obtain and / or maintain necessary equipment and skilled staff and resources to support the communication infrastructure.
3.2.12	Mission Staffing	Failure to attract, train and supply adequately experienced and qualified staff required to perform their functions effectively, especially during mission start up and liquidation periods.
3.2.13	Mission Creep	Mandated activities are exceeded by additional tasks outside the scope envisioned by the Security Council.
3.3	**International Tribunals**	
3.3.1	Investigations and Prosecution	Failure to collect sufficient evidence to support a case can result in acquittal of criminals. Transfer of cases to national courts without proper preparation can result in return of cases to the tribunal, which may not be able to handle them due to inadequate resources, ultimately resulting in inability of the tribunal to achieve its mission.
3.3.2	Trials and Appeals	Inability to undertake or complete fair and expeditious trials and appeals. Failure of the judiciary to maintain independence can result in unfair trials, acquittal of criminals, and/or prosecution of innocent individuals. Failure to observe rules of procedures and evidence in the trials and appeals process.
3.3.3	Witness Protection	Failure to provide adequate protection to witnesses leads to possible inability to try cases, ultimately resulting in inability to fulfil mission of the tribunal. Inability to monitor compliance of protection agreements with national authorities for protected witnesses.
3.3.4	Completion Strategy	Inability of the tribunals to complete trials in a fair and expeditious manner in accordance with established timeline and/or to transfer certain cases where accused persons were indicted by the tribunal to national courts.
3.3.5	Residual Capacity and Activities	Failure of the tribunal to properly plan for and execute activities that will take place after its closure or to restructure the tribunal adequately will impact its ability to achieve stated mission.
3.4	**Support Services**	
3.4.1	Funding	Failure or inability to obtain or effectively allocate funds to achieve planned programme objectives.
3.4.2	Translation and Interpretation	Failure or inability to provide accurate translation or interpretation services or outputs. Lack of sufficient and/or sufficiently skilled resources to provide required translation or interpretation services or information.
3.4.3	Procurement	Failure to purchase operating and other supplies, equipment, goods and services needed to support operations and achieve stated objectives. Inability to support organizational objectives

Risk Category		Risk Definition
Risk		
		through a coordinated and effective procurement organization, strategy and operating plan.
3.4.4	Supplier Management	Failure to maintain a system-wide registration, monitoring and evaluation process may lead the Organization to do business with less than desirable suppliers. Failure to consolidate supplier base can lead to inefficiencies and lost cost-savings.
3.4.5	Asset and Inventory Management	Failure to provide physical protection and stewardship over inventory, equipment and other physical assets, both UN and contingent owned.
3.4.6	Facilities and Real Estate Management	Failure to adequately provision, maintain and secure UN facilities.
3.4.7	Capital Master Planning	Inability to plan, manage and complete capital projects within established deadlines, budget parameters and specifications. Failure to effect a capital plan that is aligned with UN objectives. Failure to adequately plan, fund and control change orders and budget overruns.
3.4.8	Business Continuity	Inability to recover from, and continue uninterrupted operations in the event of extraordinary events whether natural events (pandemic, fire, earthquake, tsunami, tornado, etc.) or terrorist activities or other malicious acts or war.
3.4.9	Commercial Activities	The provision of commercial activities, i.e. providing services for fees, to outside parties that are incongruent with the UN's objectives and mandates (e.g., selling software or other services to third parties outside the UN system) and therefore lead to legal exposure.
3.4.10	Legal Aid	Failure to properly evaluate needs of indictees, leading to inadequate allocation of resources and ultimately, to inability to provide aid to indictees who cannot pay for their own defence, affecting their right to fair process.
3.4.11	Court Management and Legal Support	Inability to manage activities and services for the court (including inadequate management of dossiers, court schedule, organization of hearings, facilities, coordination of court services) affect the completion of trials, appeals, and/or transfer of cases to national courts.
3.4.12	Detention Unit Management	Detainee(s) are not deemed fit for trial affecting the tribunal's reputation and its ability to achieve its mission. Failure to allow those detained access to their basic human rights (e.g. living environment, healthcare, communication, to prepare their defence, protection against threats) whilst being denied their freedom.
3.5	**Human Resources**	
3.5.1	Resource Allocation and Availability	Failure to identify and prioritize staffing requirements. Inability to effectively deploy and/or allocate resources when and where they are mostly needed.
3.5.2	Recruiting, Hiring and Retention	Failure to source, identify, hire and/or retain qualified employees that ensure optimal staffing levels in a balanced workforce environment. Failure to establish processes that support replacement or fulfilment of critical positions. Examples:

Risk Category		Risk Definition
Risk		
		– Inability to identify and develop qualified candidates to fill critical roles in the event of a vacancy – Failure to attract and retain qualified employees due to work location (e.g., high cost of living, poor educational system, inadequate recreational opportunities, etc.) – Inability to hire qualified individuals due to strict allocation requirements by country, region, gender, etc. – Inability to hire qualified individuals when needed due to lengthy recruiting process
3.5.3	Succession Planning and Promotion	Failure to adequately plan for the departure of certain employees and sustain operations with minimal interruptions, e.g. the inability to develop internal resources to fill senior management positions.
3.5.4	Conduct and Discipline	Inability to sustain transparency and accountability in staff conduct and behaviour due to insufficient or non-existent disciplinary procedures. Inability to pursue disciplinary action and/or lack of consistency in its application.
3.5.5	Development and Performance	Inability to develop and enhance staff skills and provide effective performance feedback and guidance.
3.5.6	Compensation and Benefits	Inability or failure to assess and develop a compensation structure (base salary, annual/long-term incentive, benefits/perquisites) that recognises different professional skills, is adjusted adequately to reflect the cost-of-living in different locations, and is aligned with organizational needs and objectives. Compensation is not seen to reward: (1) performance (but rather seniority), (2) risk taking (but rather risk avoidance), (3) accepting mandates in crisis countries/difficult environments, or (4) skills that are in demand.
3.5.7	Medical Services	Inability or failure to provide health care services, to protect, promote and monitor health of staff.
3.5.8	Safety and Security	Inability or failure to provide a secure working environment and to protect, promote and monitor personal safety of staff, volunteers and others at UN facilities or in support of UN and related activities. Inappropriate system for co-financing security globally and inadequate governance system Local security conditions can jeopardize the safety of UN staff and the delivery of services. Overly restrictive security rules can negatively impact humanitarian endeavours. Non-compliance with UN-established safety and security guidelines.
3.5.9	Training	Failure to appropriately train UN personnel (staff, volunteers, troops, etc.) to perform or fulfil their duties and responsibilities.
3.5.10	Mobility	Inability or failure to develop and maintain a mobile workforce. Failure to balance and align the need to mobilise resources with the need to maintain certain levels of expertise within a Department, Office, Commission or location.

Risk Category		**Risk Definition**
Risk		
3.6	**Intellectual Property**	
3.6.1	Knowledge Management	Knowledge across the Organization is not captured, updated, protected, monitored and utilized in an appropriate, efficient and effective way and / or is concentrated on a few key people.
3.6.2	Information and Document Management	Records, conference documents, and mailings (paper or electronic) may not be readily available, properly produced, secured, managed and/or retained. Lack of a consistent document retention strategy or policy.
3.7	**Information Resources and Information Technology (IT)**	
3.7.1	IT Strategy and System Implementations	IT strategies, including system development and infrastructure within the Departments and Offices, are not aligned with the overall strategy and operating objectives of the Organization, nor appropriately coordinated. Lack of effective systems' integration or a defined IT strategy.
3.7.2	IT Security and Access	Failure to adequately restrict access to information (data or programmes) may result in unauthorized knowledge or use of confidential information. Overly restricted access to information may preclude personnel from performing their assigned responsibilities effectively and efficiently. Failure of Information systems to adequately protect the critical data and infrastructure from theft, corruption, unauthorized usage, viruses, or sabotage.
3.7.3	IT Availability and Continuity	The inability to recover from, and continue uninterrupted operations in the event of extraordinary events and system failure.
3.7.4	IT Integrity	Information systems that do not provide reliable information when it is needed or perform so slowly that operations are not efficient.
3.7.5	IT Infrastructure & Systems	IT infrastructure and systems do not support the information and workflow needs of the Organization, hindering its ability to efficiently and effectively meet its goals and objectives.
4. COMPLIANCE – Relating to the Organization's compliance with applicable laws and regulations, prescribed practices or ethical standards		
4.1	**Legal**	
4.1.1	Contract	Entering into contracts that are unfavourable to the Organization and/or the failure to comply with and monitor contract terms to protect the Organization. Failure to identify legal risks posed by commercial activities that lead to increased legal exposure.
4.1.2	Intellectual Property	Failure to create, capture, enhance, leverage and protect the collective knowledge, expertise and ideas.
4.1.3	Anti-Corruption	Failure to create an environment that opposes corruption and instils practices that prevent

Risk Category		Risk Definition
Risk		
		corruption may impact the UN ability to achieve its mandated objectives.
4.1.4	International Law	Inability to monitor, react and comply with International Laws and regulations, resulting in violations and loss of trust and support.
4.1.5	Privacy	Failure to identify legal risks posed by, and prevent non-compliance with, privacy laws resulting in improper disclosure of confidential information and litigation and liability exposures.
4.2	**Regulatory**	
4.2.1	Internal Policies and Resolutions	Failure to monitor, react and comply with internal policy, procedures and resolutions, resulting in litigation and liability exposures. Lack of consistency in sanctions in instances of non-compliance with rules and regulations.
4.2.2	UN Labour Relations	Failure to identify and prevent risks posed by UN regulatory requirements for labour rules and regulations
4.2.3	Host Country Regulations	Failure to comply with applicable national laws and regulations that affect relations with host countries.
5. FINANCIAL – Related to effective and efficient use of the Organization's financial resources, and reliability of Organization's reporting		
5.1	**Funding and Investments**	
5.1.1	Financial Contributions	Failure to obtain financial contributions may impede the progress of programs or initiatives. Failure to obtain financial contributions may impede payments to settle payables to Member States, such as troop contributing countries.
5.1.2	Extra-budgetary Funding	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 are given higher priority.
5.1.3	Trust Funds – Receipt of Cash	Failure to predict amounts of contribution for the long term can impact long term strategic planning. Shortfalls in the receipt of cash or expected cash flows (or timing variances) hinder programme implementation and achievement of objectives.
5.1.4	Trust Funds Management	Inability to identify, establish and maintain the optimal structure and controls for trust funds resulting in loss or misuse of assets.
5.1.5	Donor Fund Management and Reporting	Failure to meet the requirements and obligations specified by donors resulting in loss of confidence in the UN abilities to meet the desired objectives. Cost of meeting Donor reporting and other requirements for earmarked funds outweighs the programme support costs provided.

Risk Category		**Risk Definition**
Risk		
5.1.6	Cash Management	Failure to secure, administer, monitor, and manage cash related activities.
5.1.7	Investments	Poor investments practices and/or non-compliance with investment policies resulting in loss of principal investments. Management does not have sufficient financial information to make informed short-term and long-term investment decisions.
5.1.8	Financial markets	The risk that movements in prices, interest rates, indices, etc. threaten the value of the Organization's financial assets. Depreciation of the US dollar adversely affects the purchasing power of the Organization, and leads to increases in requests for budgetary allocations.
5.1.9	Insurance	Insurance coverage fails to protect the UN from significant financial losses due to incidents and claims.
5.2	**Accounting and Reporting**	
5.2.1	Financial Management and Reporting	Failure to accurately record, manage, report and present financial results periodically/timely in accordance with UNSAS/IPSAS and organizational guidelines.
5.2.2	General Accounting	Failure to process and account for transactions accurately, completely, timely, in the proper period and in accordance with UNSAS/IPSAS.
5.2.3	Financial Controls	Failure to identify and react effectively to errors, omissions or misstatements. Information concerning evaluation of internal controls do not meet UN standards, are incorrect or inconsistent or are communicated through inappropriate channels.
5.2.4	Liability Management and Disbursements	Failure to properly process, record and recognize payables accurately and timely and to process payments/distribute cash efficiently to authorized operations, programs, partners and supporters.
5.2.5	Staff Tax Reimbursements	Failure to process staff tax reimbursements timely and/or accurately.

--- ----- ---