UNITED NATIONS NATIONS UNIES

Enterprise Risk Management and Internal Control Policy

May 2011

Table of Contents

Annex

Enterprise Risk Management and Internal Control Policy

I. Introduction

The United Nations faces a considerable level of risk owing to the complexities of its operations and increased scope of its mandates. Risk management is therefore an area already considered at various levels, and embedded in different processes and operations of the United Nations Secretariat. Capital Master Plan[1], Information and Communication Technology[2], Security[3], Organizational Resilience[4], among other areas, have already successfully adopted and implemented risk management methodologies and practices.

The General Assembly fully recognized the importance of the implementation of a systematic approach to risk management and internal control in the United Nations, and provided a clear mandate to the Secretary-General to enhance "the current capabilities in the Secretariat responsible for risk assessment and mitigation and internal control on the basis of [...] annex II to the report of the Secretary-General [A/64/640]"[5].

Following the mandates of the General Assembly, and fully in line with the benchmarks on enterprise risk management implementation recommended by the Joint Inspection Unit ("JIU")[6], this Policy further expands and strengthens the approach to risk management already embraced by different areas of the Organization, adopting an integrated Enterprise Risk Management and Internal Control Framework ("the framework") that provides a consistent and comprehensive risk management methodology that can be applied across the entire Secretariat.

Given the operational nature of the work of the Organization and the resultant broad array of its activities, the framework allows for a strong operational component, and outlines a flexible structure which can be easily adhered to across the spectrum of activities and work environments, without resulting in additional administrative overhead for staff members.

The Secretary-General strongly believes enterprise risk management is the inherent core responsibility of management. With the adoption of an enterprise risk management and internal control process as a strategic initiative, the Secretariat defines a consistent methodology for assessing, treating, monitoring and communicating risks. The framework is designed to 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, defining a flexible methodology that is fully compatible with the different risk management practices already adopted by the Organization,

[1] "Capital Master Plan Risk Management Framework", April 2008.
[2] Adoption of ISO 27001, ISO 27002 and Octave Risk Assessment Methodology by the Information and Communications Technology Board of the Secretariat, April 2008.
[3] "Policies and Guidelines on Security Risk Management and Minimum Operating Security Standards", April 2009.
[4] "Organizational Resilience Policy for the United Nations Headquarters, New York", June 2010.
[5] Resolution A/RES/63/276 of 26 June 2009 and Resolution A/RES/64/259 of 5 May 2010.
[6] "Review of enterprise risk management in the United Nations system: Benchmarking framework", JIU/REP/2010/4, Joint Inspection Unit, 2010.

e.g. with regard to security risks. Properly implemented, it provides insight into potential risks as well as new opportunities, and shall become a key part of the strategy and planning processes.

II. Definition

Consistent with the best international standards[7] 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 applied in strategy-setting throughout the Organization.

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.

III. Purpose

The Secretary-General is convinced that the implementation of this framework will 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

[7] "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.

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 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.

IV. Principles

The enterprise risk management and internal control programme 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 project, 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, treatment, 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. Risk management shall be in particular 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 ("ACABQ") and the IAAC, as may be relevant, will be then in a position to effectively fulfil its responsibilities of determining the risk tolerance of the Organization.

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.

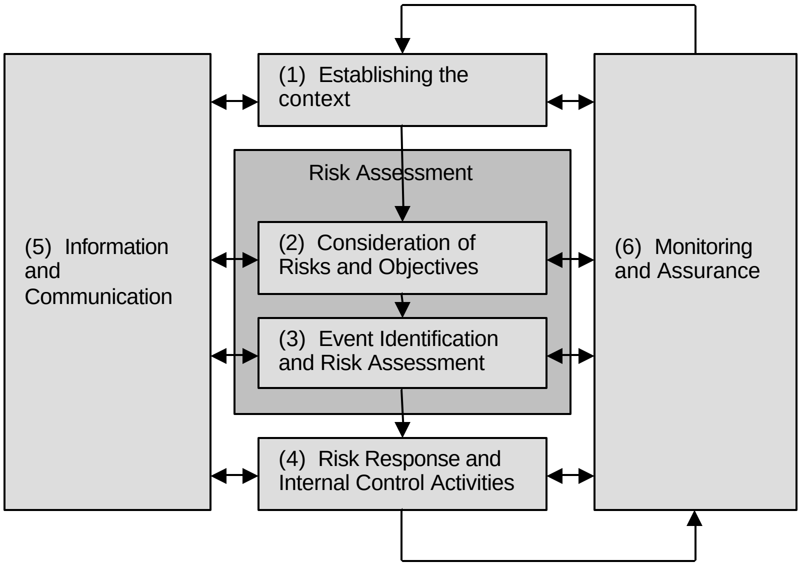
(ii) **Accountability** – The adoption of an effective framework relies on the full ownership and accountability of management at each level throughout the Organization for risk management and internal control activities.

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

V. Process

Enterprise risk management, as defined before, 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 the Annex of this Policy – 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 risk exposure. 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, analysis of historical data, and other sources. Identified risks shall then be measured and scored according to the weighting of perceived impact, likelihood and level of internal control effectiveness. Once the assessment is completed, the ability to appropriately link risks to both organizational strategies and objectives, and the underlying processes and activities, is critical to the identification and implementation of effective risk mitigation measures.

(4) **Risk Response and Internal Control Activities** – Consistent with the methodology adopted by the Office of Internal Oversight Services[8], the risk assessment shall consider existing key controls in addition to inherent risks, resulting in the identification of residual risks. 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. 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, supported by adequate information systems. 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, and of the necessary tools, is provided in the *Enterprise Risk Management and Internal Control Methodology* paper, that complements this Policy.

VI. Risk Governance Structure, Roles and Responsibilities

Proper risk governance mechanisms are critical for the adoption of an effective risk management framework. This section provides a description of the roles and responsibilities of the different functions involved, followed by an illustration of the risk management and internal control governance structure (Figure 2).

General Assembly

The General Assembly, with the advice of the ACABQ and IAAC, is responsible for determining the risk tolerance of the Organization[9].

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.

[8] "Activities of the Office of Internal Oversight Services for the period 1 July 2010 to 30 June 2011", A/66/286, 9 August 2011.

[9] "Resolution adopted by the General Assembly – Progress towards an accountability system in the United Nations Secretariat", A/RES/66/257, 12 April 2012.

Management Committee

The Management Committee, acting as Enterprise Risk Management Committee for the Secretariat, annually reviews the results of the risk assessments at entity level, and has an active role in the promotion of the best practices in risk and internal control management in the Organization, involving other Committees, 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.

Local Risk and Internal Control Focal Points

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 be 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.

As recommended by benchmark 4 of the JIU review of enterprise risk management in the United Nations system[10], an Enterprise Risk Management and Internal Control function shall assist senior management in the process of establishment of the described framework, and provide the appropriate level of implementation and execution oversight.

The 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 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.

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[11].

The main responsibilities of the Enterprise Risk Management and Internal Control function shall involve, amongst other matters:

(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.

(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.

[10] Paragraph 84 and 88, “Review of enterprise risk management in the United Nations system: Benchmarking framework”, JIU/REP/2010/4, Joint Inspection Unit, 2010.

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

(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 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.

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. All staff members, in accordance with their specific role and function, must embed risk management in operational decision making, identifying, managing and monitoring risks with regard to day-to-day operations within their respective areas of responsibility.

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.

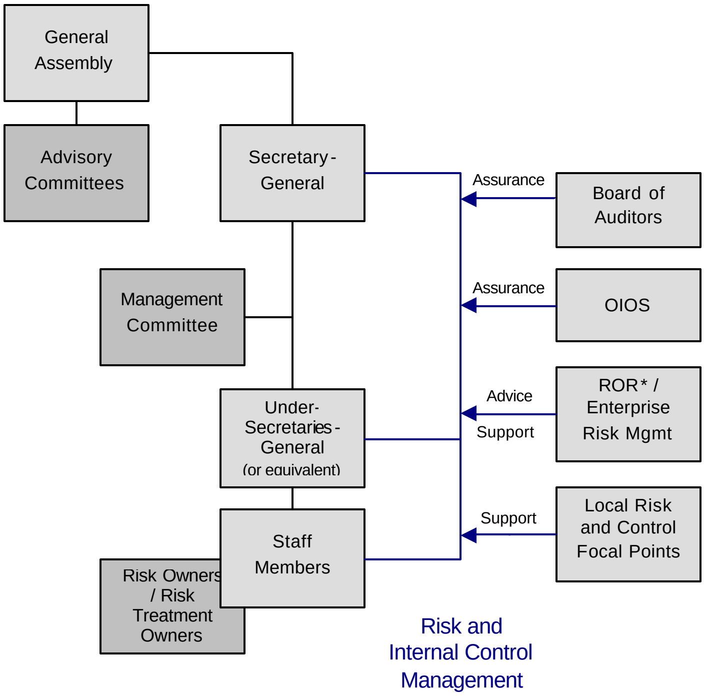
Joint Inspection Unit

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[12].

Figure 2 - Risk and internal control management governance


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

*High level official responsible for risk within the Organization

[12] "Financial Regulations and Rules of the United Nations", Article VII.

VII. Conclusions

This Policy defines the enterprise risk management and internal control programme that is formally implemented within the United Nations Secretariat to allow the Organization to improve its accountability and decision making process. The adoption of this Policy and the maintenance of an enterprise risk management and internal control process shall provide reasonable assurance as to the Organization's ability to effectively achieve its mandates and objectives.

The Policy, as complemented by the Methodology describing the activities to be performed for the effective implementation of the enterprise risk management and internal control framework, shall be individually applied to each Department, Office, Commission, Mission, or Tribunal according to the level and context of risk and risk assessment, and shall be reviewed for effectiveness on an ongoing basis. It is the responsibility of management to comply with this Policy and related procedures.

It shall be noted that the full implementation of this Policy and of the Methodology will require the establishment of a centralized dedicated capacity for Enterprise Risk Management and Internal Control within the Secretariat, supported by an adequate level of resources, as recommended by the JIU review of enterprise risk management in the United Nations system[13].

[13] JIU/REP/2010/4.

Annex

Glossary of Terms and Definitions[14]

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 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.

Residual Risk

The remaining risk after management has taken action to alter the risk's likelihood or impact.

[14] 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.

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.

--- ----- ---