IUCN Enterprise Risk Management Policy

Annexes

INTERNATIONAL UNION FOR CONSERVATION OF NATURE

Cover photo: Los Glaciares National Park (Argentina) © Philipp Schinz

IUCN
Rue Mauverney 28
1196 Gland, Switzerland
Tel: +41 22 999 0001
Fax: +41 22 999 0020
http://www.iucn.org

TABLE OF CONTENTS

ANNEX 1 IUCN RISK MANAGEMENT ROLES AND RESPONSIBILITIES 2
ANNEX 2 IUCN ERM RISK TAXONOMY 3
ANNEX 3 IUCN ERM CRITERIA MODEL DETERMINING LIKELIHOOD AND IMPACT 5
ANNEX 4 RISK APPETITE STATEMENT 8
ANNEX 5 OPERATIONAL GUIDELINES 11
ANNEX 6 TERMS OF REFERENCE – RISK MANAGEMENT COMMITTEE 15

ANNEX 1 IUCN RISK MANAGEMENT ROLES AND RESPONSIBILITIES

The following table outlines the main roles and responsibilities with respect to risk management and internal control.

IUCN	MAIN ROLES AND RESPONSIBILITIES
COUNCIL	Provides policy oversight and review of Enterprise Risk Management.
FINANCE AND AUDIT COMMITTEE (FAC)	Performs regular review of Enterprise Risk Management activities. Advises IUCN Council on the effectiveness of risk management.
DIRECTOR GENERAL	Drives a culture of risk management and is accountable for the implementation of the IUCN [Enterprise] Risk Management Policy. Sets and/or approves the overall risk appetite and risk tolerances
EXECUTIVE BOARD	Ensures Directors and Heads of Units comply with IUCN Enterprise Risk Management Policy, including by fostering a culture where risks can be identified and escalated. Decides resource allocation for strategic risk treatment. Accountable for adherence and countermeasures.
RISK MANAGEMENT COMMITTEE	Reviews and analyses strategic corporate risks, aggregated risk registers, and escalated risks from regions, centres and units. Monitors, reviews and maintains the overall risk framework. Proposes to the Executive Board corresponding treatment, where required.
DIRECTORS/COMMISSIONS CHAIRS/HEADS OF UNITS	Owns the risks with accountability for and authority to manage the risk. Registers risks in timely and accurate manner. Leads overall coordination for assessing and effectively mitigating risk. Ensures operations are carried out within the limits of acceptable risks (risk appetite).
PROGRAMME PERFORMANCE, MONITORING AND EVALUATION UNIT	Continuously improves supporting procedures and guidance. Coordinates and prepares Risk Management Committee meetings and documents, including horizon scanning. Collects, aggregates and analyses corporate risks. Leads internal control self-assessment exercise. Leads capacity-building activities for risk management.
REGIONAL PROGRAMME COORDINATORS/MONITORING EVALUATION and LEARNING COORDINATORS/PROGRAMME OFFICERS/PROJECT MANAGERS	Owns and manages the risks. Registers monitors and reports risks in a timely and accurate manner, in accordance with institutional guidelines and requirements. Implements mitigation measures and monitor risk. Complies with IUCN Enterprise Risk Management policy and supporting procedures and guidance.

ANNEX 2 IUCN ERM RISK TAXONOMY

A risk taxonomy is a comprehensive set of risk categories and sub-categories comprising of indicative granular events used within IUCN to help those involved in the risk identification process. The taxonomy provides:

- a common set of risk categories and sub-categories, which facilitates the aggregation of risks from across the different levels within IUCN and the prioritisation of mitigation activities;
- a stable set of risk categories and sub-categories, which facilitates comparative analysis of risks over time;
- a risk classification system in relation to what IUCN does to help to systematically identify and track the risks across its main areas of operations; and
- a comprehensive and stable set of risk categories and sub-categories, which supports the Risk Committee and Executive Board to regularly check the health of the organisation.

During the process of risk identification, the use of the taxonomy is a mandatory requirement.

STRATEGIC	FINANCIAL	PEOPLE MANAGEMENT	OPERATIONAL	LEGAL/ COMPLIANCE	INFORMATION SYSTEMS	EXTERNAL
Governance	**Financial sustainability**	**Staffing**	**IUCN Programme execution**	**Laws/regulations**	**IS delivery**	**Geopolitical**
– Vision, mandate – Value proposition – Foresight and vision capacity – Strategy relevance & alignment – Strategy execution & monitoring – Efficiency and effectiveness of IUCN Council and Committees – Commissions & Members engagement – Budgeting & Planning	– Funding (restricted, unrestricted) – Budget implementation – Cost recovery – Financial monitoring & reporting – Financial audit	– Strategic workforce planning – Recruitment strategy & process – Appropriate staffing	– Operational capacity & performance – Programme relevance, quality & results – Monitoring, Evaluation & Learning – Business continuity – Systems and processes – Compliance and oversight – Programme synergies	– Compliance to local law (labour) – Compliance to international laws – Anti-money laundering – Anti-bribery violations – Restrictive measure (sanctions) – Intellectual property	– Overall strategy & alignment – IS transformation execution – Performance & adoption – IS operations & service delivery – Third party	– Political & Social instability – War – Armed conflicts

Organisational efficiency & sustainability	Financial operations	Staff management	Partners	Fraud and corruption	Data & information management	Economics
– Relevance/ Efficiency – Business model – Pipeline & Portfolio management – IUCN offices legal status – Organisational development	– Investment – Treasury management – Asset management – Accounting systems – Payroll management – Travel management – Accounts payable – Procurement	– People management & leadership skills – Staff development & upskilling – Employee turn-over – On boarding – Performance management	– Execution capacity – Implementation arrangements – Due Diligence – Contracting – Compliance	– Bribery – Misuse of assets – Conflict of interest – Code of conduct	– Data Governance – Data availability & Data quality – Inability to trace information – Business intelligence	– Macroeconomic events – Fiscal crises – Foreign exchange – Legal changes
Transformation & change		**Staff health, security & safety**	**Communication & reputation**	**Donor compliance**	**Data protection & IS security**	**Environmental**
– Innovation culture & capacity – Capacity & agility to absorb internal & external changes		– Staff well-being – Mental health & Stress – Physical health – Environmental hazards – Transportation safety	– Reputation internal & external – Defamation of IUCN – Controversies over corporate partners or suppliers – Brand image – Public perception	– Donor requirements management – Donor fund management – Donor reporting requirements	– GDPR, data breach – Data protection – Cyber security	– Environmental events

NOTE: The ERM Risk Taxonomy will be updated according to changes in IUCN Risk Profile.

ANNEX 3 IUCN ERM CRITERIA MODEL DETERMINING LIKELIHOOD AND IMPACT

The purpose of the risk assessment process is to assess the likelihood (probabilities) and impact (consequences) of the identified risks. The likelihood levels are described as qualitative level. The impact levels are described in terms of both qualitative and quantitative level. The results of this assessment are then used to prioritise risks, compare them against the risk appetite and to identify treatments.

If the estimation of the likelihood and/or the impact remain difficult, a cautious approach is recommended by estimating the highest rating to ensure the risk is treated accordingly and closely monitored.

IUCN's methodology for determining likelihood and impact at project level is an adapted version of the Project Management Institute methodology, which sets international standards for project management.[1]

DETERMINING LIKELIHOOD

For project, the IUCN ERM Policy identifies several degrees of likelihood (probabilities) on a four-point scale for project:

LIKELIHOOD	UNLIKELY	POSSIBLE	LIKELY	ALMOST CERTAIN
	1	2	3	4
DESCRIPTION ("THE RISK IS EXPECTED TO MATERIALISE.")	Low probability to occur	Medium-Low probability to occur	Medium-High probability to occur	High probability to occur

DETERMINING IMPACT

Impact is also ranked on a four-point scale. When determining the overall impact, the IUCN ERM Policy identifies several types of impact (consequences) that should be considered.

For project level, these consequences are those related to budget, operations, delivery and schedule. Although written in similar language and using similar tools, and whilst one can be impacted by the other, IUCN applies a simplified set of impact at project level. For Regional/Centre/Commissions/Unit/Corporate levels, a more comprehensive set of impact is provided.

DETERMINING IMPACT AT THE PROJECT LEVEL

IMPACT	MINOR	INTERMEDIATE	EXTENSIVE	EXTREME
	1	2	3	4
OPERATIONAL (time)	Insignificant change	Minor delay (few weeks)	Major delay (few months)	Blockage
RESOURCES	Insignificant change	5% increase or decrease	10% increase or decrease	20% increase or decrease

[1] Project Management Institute: www.pmi.org/learning/library/risk-analysis-project-management-7070

PRODUCTS and SERVICES quality and quantity (e.g. workplans)	Insignificant quality and quantity degradation or augmentation	Minor change	Major change	Unacceptable change
RESULTS SCOPE (increase or decrease in result coverage, e.g. log frames)	Insignificant scope change deviation	Minor areas affected	Major areas affected	Unacceptable change

At the Regional/Centre/Commissions/Country/Unit/Corporate levels, each of the different impact (consequences) options presented in the below table needs to be used. The overall impact across the different consequences of a risk is then based on the highest level of impact (for example, if one of the consequences has an impact of 4, then the overall impact for that risk is 4).

DETERMINING RISK LIKELIHOOD AND IMPACT AT REGION, CENTRE, COMMISSION, COUNTRY, CORPORATE UNIT LEVELS

DESCRIPTION OF CONSEQUENCE	LIKELIHOOD	UNLIKELY	POSSIBLE	LIKELY	ALMOST CERTAIN
		1	2	3	4
	DESCRIPTION ("THE RISK IS EXPECTED TO MATERIALIZE….")	Every 4 years	Every 1–4 years	Once or twice a year	Several times a year
	IMPACT	MINOR	INTERMEDIATE	EXTENSIVE	EXTREME
		1	2	3	4
	FINANCIAL	<1% deviation from budget	1–5 % deviation from budget	5-20% deviation from budget	>20% deviation from budget
	PERFORMANCE	5–10 % of the applicable work plan	10-20 % of the applicable work plan	20-50% of the applicable work plan	>50% of the applicable work plan
	COMPLIANCE	No deviation from applicable policies and/or regulations	Moderate deviation from applicable policies and/or regulations	Significant deviation from applicable policies and/or regulations	Major deviation from applicable policies and/or regulations
	SAFETY & SECURITY	Injuries/illness not requiring medical attention and/or Local/isolated staff issue	Moderate effect on IUCN Personnel and/or Moderate impact on IUCN operations	Multiple people with serious injuries and/or security impact on operations	Deaths (single or multiple) and/or serious security impact on operations

	REPUTATION	No press exposure Localised negative comments from external stakeholders but recoverable	Negative reports/ articles in national, regional media and/or from external stakeholders but recoverable	Negative reports/ articles in several national, regional and/or international media for a period of a week or more, and/or criticism from key stakeholders	Negative reports/ articles in several national, regional and/or international media for a period of a month or more, and/or strong criticism from key stakeholders

ANNEX 4 RISK APPETITE STATEMENT

INTRODUCTION

Risk appetite is defined as the types and amount of risk, on a broad level, an organisation is willing to accept in pursuit of value (COSO standard definition). It reflects the risk management philosophy of IUCN, and in turn influences the organisation's culture, processes, and operations. Risk appetite should not be seen as a separate process but as an integral part of the risk management methodology.

IUCN's strategic objectives require ambition and ability to take planned and managed risks where these are necessary to achieve strategic outcomes. The key is to understand how much risk IUCN is willing to accept.

For IUCN to take appropriate level of risk in the risk assessment process, the IUCN Council and the IUCN Secretariat have formulated these generic risk appetite statements:

- IUCN Council expects managers of IUCN to own and manage the risks they are taking, and to pursue risk only as it is necessary and appropriate to achieve IUCN's strategic goals and/or objectives.
- IUCN's first line of defence shall establish appropriate treatments and set tolerances in their operations that reflect the risk appetite statements.

SCOPE, PURPOSE, and APPLICABILITY

This Risk Appetite Statement provides a clear framework for the IUCN Secretariat in the conduct of its operations. It also provides overarching guidance to all IUCN constituents (Council, Commissions and Member Organisations), who are strongly encouraged to apply IUCN's risk appetite and are expected to observe guidance relating to "No appetite for risk" when representing IUCN, executing IUCN projects and / or using IUCN knowledge and tools.

The purpose of this Risk Appetite Statement is to ensure that the risks that IUCN is willing to take are compatible with its capacities and ensure that they can be managed without placing the organisation at unacceptable or unmanageable levels of risk.

The Risk Appetite Statement applies to all activities undertaken by IUCN and is used in unit and project level risk registers to help steer and manage risks. It provides a clear process and guidance on the types of risks IUCN is willing to take to achieve organisational objectives.

RISK APPETITE STATEMENT

The Risk Appetite Statement is broken down in seven categories: strategic, financial, workforce and talent, operational, legal and compliance, information systems, and external.

For each category, a global risk appetite level is decided and revised annually.

Each category is further broken down in risks statements for specific areas of focus allowing for establishing a more granular appetite level to be used by IUCN staff.

A four-point appetite scale is used to determine the most appropriate risk response. The following definitions are used:

HIGH appetite: Confident risk management approach. Taking risk to maximize opportunities.

MEDIUM appetite: Conservative risk management approach. Willing to take certain amount of risk with treatments available to mitigate the risk.

LOW appetite: Cautious risk management approach. Mitigating the risk to minimise the likelihood and/or the impact.

NO appetite: Highly cautious risk management approach. Avoiding the risk.

Risk category	Risk appetite level	Statements
STRATEGIC *In keeping with its Mission Statement, IUCN's strategic planning process aims to ensure that strategic positioning, programme relevance, programme effectiveness, finances and global operations are sustainable and support programmatic delivery.*	**MEDIUM**	As a Union, IUCN has **NO** appetite for deviations from its statutes and policies, which could do damage to its values, mission, or reputation. IUCN has **NO** appetite for risks of causing harm to nature, the environment, and the people. IUCN has **HIGH** appetite for exploring innovative approaches; new fundraising activities; running ambitious projects; developing partnerships if these are in line with IUCN programme and if the benefits and opportunities outweigh the risks (otherwise, the appetite is **MEDIUM**).
FINANCIAL *IUCN must remain financially sustainable to continue to serve its purpose and achieve its vision and mission.*	**MEDIUM**	IUCN has **NO** appetite for activities that will breach financial rules, procedures and / or internal controls. IUCN has **LOW** appetite for incurring financial losses across its operations worldwide. IUCN has **MEDIUM** appetite to dedicate a certain part of funding for exploring new avenues to diversify revenue streams through partnerships with non-traditional partners and/or donors. IUCN has **HIGH** appetite to invest in opportunities and strategic initiatives that align and promote IUCN's vision and mission and are supported by robust business cases and associated financial information.
PEOPLE MANAGEMENT *IUCN should refrain from putting employees in situation where safety and security are not guaranteed. IUCN is committed to exploring strategies to attract, manage, develop and retain skilled staff to meet its strategic objectives.*	**LOW**	IUCN has **NO** appetite to deviate from its core values and standards with respect to equality, diversity, and dignity. IUCN has **MEDIUM** to **HIGH** appetite to invest and retain in its workforce through robust recruitment process, future-focused competency framework, and innovative staff management tools that are aligned with its strategic priorities and programme needs. IUCN has **LOW** appetite for operations that put staff at risk of harm. IUCN will maintain offices in locations as long as the organisation can balance the likelihood for security breaches with risk mitigations such as staff evacuation protocols and allocation of additional security resources. IUCN has **LOW** appetite for undertaking field visits in high security-risk countries and areas in accordance with IUCN Global Safety and Security Policy.

OPERATIONAL *IUCN must have comprehensive operational systems, practices and partnerships that support the achievement of its strategic objectives. IUCN implements its strategic objectives through a diverse and large global and regional programme and project portfolios.*	**MEDIUM**	IUCN has **NO** appetite to collaborate with partners that are not in alignment with IUCN values and policies (e.g. Code of Conduct and Professional Ethics, Policy on the Protection from Sexual Exploitation, Sexual Abuse, and Sexual Harassment). IUCN has **MEDIUM** appetite for implementing and executing ambitious projects when aligned with its programme and portfolio strategic priorities. Rigorous programme and project management standards must be applied at all times. IUCN has **MEDIUM** appetite when engaging with new partners for implementing activities or delivering new services and products to continually improve IUCN presence, expertise and value proposition. These partners must successfully pass the institutional due diligence process.
LEGAL & COMPLIANCE *IUCN adheres to relevant statutory and policy requirements in all locations where IUCN operates.*	**NO**	IUCN has **NO** appetite for non-compliance with relevant IUCN's statutory and policy requirements in all locations where IUCN operates. IUCN has **NO** appetite for misconduct, harassment or discrimination and non-compliance behaviour that undermines the integrity of IUCN. IUCN has **NO** appetite for risks such as fraud, unethical conduct, or non-compliance with legislation that could impact our reputation and stakeholder confidence.
INFORMATION SYSTEMS *IUCN embraces technological innovations while being equipped with innovative security and IS delivery.*	**LOW**	IUCN has **NO** appetite for non-compliance with relevant data protection regulations in the countries where IUCN operates. IUCN has **LOW** appetite for risks that could affect IS infrastructures, business operations productivity or system downtime. IUCN has **MEDIUM** appetite while adopting innovative technologies to drive practices that are more efficient and to support programme innovation.

ANNEX 5 OPERATIONAL GUIDELINES

In respect to the ERM methodological steps, outlined in IUCN ERM Policy section 4.2, Pillar 2, the following guidelines describe the operational steps and requirements to follow for each level of IUCN. These steps include the frequency, the actions items and the person accountable and involved in each step of the risk management process.

GUIDELINES FOR MANAGING RISK AT PROJECT LEVEL

	Communication & Consultation	Scope, Context & Criteria	Risk Assessment *(Identify, analyse, evaluate)*	Risk Treatment	Risk Monitoring & Review	Risk Recording & Reporting
When	Throughout project life cycle	At concept stage	At design stage *(further refinement at proposal development)* and during implementation	Connected to risk assessment step	On a quarterly basis	On a yearly basis *(in line with annual strategic planning and monitoring cycle)*
What	• Engage and consult with relevant staff and partners on risk management process. • Keep staff and partners informed on risk management processes at project level.	• Integrated in project documents (e.g. work plan, theory of change, donors requirements etc.) • Analyse internal and external project context where activities are planned. • PESTLE and/or SWOT methodologies can be used for this step.	• Identify risks during conception and as often as needed during implementation risks using IUCN taxonomy. • Evaluate risks applying the ERM criteria model • Evaluate each risk with risk appetite to determine which risks can be accepted, and those requiring treatment. • Use relevant risk register to record risks.	• Treatment identification and ownership in risk register during project conception, prior to project approval. • During implementation, update/confirm risk treatment measures to address changes in context, new information and new risks. • Implement identified risk treatment if needed. • Escalate/transfer risks that meet any escalation conditions to line management.	• Update risk register to highlight any risk movement and/or inclusion of new risk. • Scanning of changing internal and external context, reflecting on how risk levels may be changing, identifying emerging risks. • Monitor progress and relevance of risk treatment measures.	• Risks recorded and reported through the risk register, and shared with project stakeholders and PPME unit for portfolio consolidation. • Report to donors and external audit as needed.
Who	Project manager + Staff and Partners	Project manager + Staff and Partners	Project manager + Staff and Partners	Project Manager + Risk Owners	Project Manager + Risk Owners	Project Manager

GUIDELINES FOR MANAGING RISK AT PORTFOLIO LEVEL

	Communication & Consultation	Scope, Context & Criteria	Risk Assessment *(Identify, analyse, evaluate)*	Risk Treatment	Risk Monitoring & Review	Risk Recording & Reporting
When	Throughout portfolio lifecycle	On a quarterly basis (*Informed by project- level risk registers*	Carried out once a year *(in line with annual strategic planning and monitoring cycle)*	Connected to risk assessment step	On a quarterly basis	On a yearly basis *(in line with annual strategic planning and monitoring cycle)*
What	• Engage and consult with project managers, regional programme coordinators, MEL Coordinators on risk management process. • Keep project managers, regional programme coordinators, MEL coordinators informed on risk management processes at the portfolio level.	• Informed by respective risk data on a quarterly basis and by the consolidation of projects' risk registers on an annual basis. • Analyse internal and external portfolio context • PESTLE and/or SWOT methodologies can be used for this step.	• In consultation with relevant stakeholders, identify risks using IUCN taxonomy for the portfolio objectives. • Evaluate risks applying the ERM criteria model. • Evaluate each risk with risk appetite to determine which risks can be accepted, and those requiring priority treatment. • Use relevant risk register to record risks.	• Treatment identification and ownership in risk register. • During implementation, update/confirm risk treatment measures to address changes in context, new information and new risks. • Implement identified risk treatment if needed. • Escalate/transfer risks that meet any escalation conditions to line management.	• Use project performance, financial and risk information. • Scanning of changing internal and external context, reflecting on how risk levels may be changing, identifying emerging risks. • Monitor progress and relevance of risk treatment measures.	• Risks recorded and reported through the portfolio risk register. • Portfolio risk profile is discussed with management and inform Regional/Centre risk registers. Shared with PPME for global portfolio consolidation.
Who	Portfolio Manager + relevant staff	Portfolio Manager + relevant staff	Portfolio Manager + relevant staff	Portfolio Manager + Risk Owners	Portfolio Manager + Risk Owners	Portfolio Manager

GUIDELINES FOR MANAGING RISK AT REGION, CENTRE, COMMISSION, COUNTRY, CORPORATE UNIT LEVELS

	Communication & Consultation	Scope, Context & Criteria	Risk Assessment *(Identify, analyse, evaluate)*	Risk Treatment	Risk Monitoring & Review	Risk Recording & Reporting
When	As often as appropriate	Twice a year	Twice a year *(Integrated with annual strategic planning and monitoring cycle)*	Connected to risk assessment step	Twice a year	Twice a year *(Integrated with annual strategic planning and monitoring cycle)*
What	• Engage and consult with country representatives, regional programme coordinators, team leads, corporate staff, on risk management process. • Keep stakeholders informed on risk management processes at the portfolio level.	• Informed by relevant portfolio risk registers. • Integrated in Regional/Centre/ Programme/ Corporate Units work plans. • PESTLE and/or SWOT methodologies can be used for this step.	• In consultation with relevant stakeholders, identify risks using IUCN taxonomy. • Analyse likelihood and impact by applying the ERM criteria model. • Evaluate each risk with risk appetite to determine which risks can be accepted, and those requiring priority treatment. • Use relevant risk register to record risks.	• Treatment identification and ownership in risk register. • Respond to escalated risks. • Escalate the risks that cannot be adequately addressed to Risk Committee.	• Scanning of changing internal and external context, reflecting on how risk levels may be changing, identifying emerging risks. • Monitor progress and relevance of risk treatment measures • Captured as part of the annual strategic planning and monitoring exercise (annual cycle). Combined with the risk monitoring done at portfolio level.	• Risks recorded and reported through the relevant risk register. • Risk registers are discussed with senior management and inform Corporate Risk Register.
Who	Regional Directors Centre Directors Commission Chairs Heads Corporate Units + Stakeholders	Regional Directors Centre Directors Commission Chairs Heads Corporate Units + Stakeholders	Regional Directors Centre Directors Commission Chairs Heads Corporate Units + Stakeholders	Regional Directors Centre Directors Commission Chairs Heads Corporate Units + Risk Owners	Regional Directors Centre Directors Commission Chairs Heads Corporate Units + Risk Owners	Regional Directors Centre Directors Commission Chairs Heads Corporate Units

GUIDELINES FOR MANAGING RISK AT CORPORATE LEVEL

	Communication & Consultation	Scope, Context & Criteria	Risk Assessment *(Identify, analyse, evaluate)*	Risk Treatment	Risk Monitoring & Review	Risk Recording & Reporting
When	As often as appropriate	Twice a year	Twice a year *(Integrated with annual strategic planning and monitoring cycle)*	Connected to risk assessment step	Twice a year *(Integrated with annual strategic planning and monitoring cycle)*	Twice a year *(Integrated with annual strategic planning and monitoring cycle)*
What	• Engage and consult with Risk Committee members on risk management process • Communicate IUCN risk management activities to the Risk Committee and Executive Board through annual reporting cycle.	• Provided by Regional, Centres, Countries, Units and Portfolio risk analysis • Provided by foresight report incorporating macro trends that may affect IUCN risk profile. • Provided by analysis of the internal control self-assessment (Biannual).	• Identify, using IUCN taxonomy, major risks at corporate level affecting IUCN. • Analyse likelihood and impact by applying the ERM criteria model. • Evaluate risk in the corporate risk register to define the risks that require priority treatment based on IUCN's risk acceptance to meet its objectives. • Use relevant risk register to record risks.	• Treatment identification and ownership in risk register. • Escalate the risks from Regions, Centres and Units for consideration by the Risk Committee to make decisions on escalated corporate risks (prioritise and take specific actions). • Propose to the Executive Board corresponding treatment, where required.	• Captured as part of the annual strategic planning and monitoring exercise (annual cycle). • Involves constant scan of the changing internal and external context, reflecting on how risk levels may be changing, identifying emerging risks. • Monitor progress and relevance of risk treatment measures	• Risks recorded and reported through the corporate risk register. • Report the overall risk profile of IUCN to the Risk Committee, Executive Board and FAC. • Report to donors and external audit risk management framework
Who	Risk Committee + PPME	PPME + Risk Committee	Risk Committee	Risk Committee + Risk Owners	Risk Committee + Risk Owners	PPME + Risk Committee

ANNEX 6 TERMS OF REFERENCE – RISK MANAGEMENT COMMITTEE

INTRODUCTION

IUCN's Enterprise Risk Management framework guides the conduct and application of ERM and defines roles and responsibilities. At the corporate level, the Risk Management Committee –serves as the main platform to identify, assess, develop treatment and monitor risks at the corporate level. The Committee is chaired by the Deputy Director General Corporate Services who oversees the overall implementation and use of the ERM framework in IUCN. The Risk Management Committee is a sub-committee of the Executive Board and reports to the Executive Board on the framework on a semi-annual basis.

DUTIES AND RESPONSIBILITIES

In line with the relevant policy(ies), the Risk Management Committee is responsible for:

REVIEWING AND ANALYSING CORPORATE RISKS

Embedded in the Strategic planning and reporting framework and on a semi-annual basis, a risk analysis, including regional, centre and portfolio risk information is prepared by PPME and brought to the attention of the Committee. The analysis is then scanned for possible emerging risks and/or risks with increasing criticality that might require corporate level treatments. This analysis, when applicable, might include the comparison between risks logged in the respective risk register and risks that materialised within the reporting period.

Under this responsibility, the Committee will:

- Review corporate, units and portfolio risks and progress of mitigation actions;
- Review, deliberation and treatment plan of escalated risk;
- Propose strategy and resource allocation for risk treatment to the Executive Board; and
- Address those risks escalated to the Committee.

MONITORING, REVIEWING AND MAINTAINING THE OVERALL RISK FRAMEWORK

Under this responsibility, the Committee performs monitoring and review functions and, more generally, ensures the maintenance of the ERM framework itself in line with industry standards. In doing so, the Committee continuously ensures the appropriateness of the risk criteria, analysis, treatment and the framework itself.

In performing their responsibilities, the Committee will:

- Ensure that relevant guidance and other supporting material is updated;
- Recommend changes in the ERM Policy and other relevant policies, in line with the level of maturity of the organisation's systems and processes;
- Ensure risk registers at all levels of the Secretariat are fully operational, standardised and integrated;
- Ensure internal controls are in place and reviewed periodically;
- Develop, facilitates and grows a network of in-house experts in risk management;
- Build and disseminate knowledge, including by promoting ways for capturing, reviewing lessons learned and best practices; and
- Ensure training of staff is available.

COMMITTEE MEETINGS TIMEFRAME AND STANDING AGENDA

The Committee meets on a semi-annual basis in line with the Strategic Planning and Reporting Framework. On an ad-hoc basis, the Chair of the Risk Management Committee can also call for a committee meeting for immediate deliberation of an urgent risk issue. The standing agenda for the Committee meeting is as follows:

- Opening remarks from the Chair;
- Review of corporate, units and portfolio risks and progress of mitigation actions;
- Risk escalation with treatment proposal to the Executive Board;
- Discuss the effectiveness of the enterprise-wide risk framework and recommend improvements;
- Internal controls self-assessment review (every two years);
- Risk Appetite Statement review/validation (yearly); and
- Any other business.

RISK COMMITTEE MEMBERS

The Committee is comprised of the following members:

- DDG Corporate Services (Chair);
- Centre Director (one);
- Regional Director (one);
- Chief Financial Officer;
- Head of Oversight;
- Head, PPME; and
- Risk and Accountability Officer.

On an ad-hoc basis, the Committee might invite other staff to sit in its meetings to deliberate on specific issues. This might include:

- Risk owner of specific corporate risk entries;
- Line manager of specific unit;
- Expert or resource persons on a particular issue; and
- Other staff as necessary.

The Programme Performance, Monitoring and Evaluation Unit assists the Chair and Committee members in effective and efficient management of committee meetings. This includes:

- Preparing agenda and background materials for Committee meetings;
- Recording and presenting escalated risks for Committee deliberations;
- Ensuring proper documentation of Committee decisions;
- Recording and sharing minutes of the meetings; and
- Any other tasks as assigned by the Chair of the Committee.

INTERNATIONAL UNION
FOR CONSERVATION OF NATURE
Rue Mauverney 28
1196 Gland,
Switzerland
www.iucn.org