RAINFOREST FOUNDATION NORWAY

RISK MANAGEMENT POLICY

RAINFOREST FOUNDATION NORWAY RISK MANAGEMENT POLICY

Policy owner:
Senior Management Team

Policy lead:
Organisational Director

Adopted: April 2021

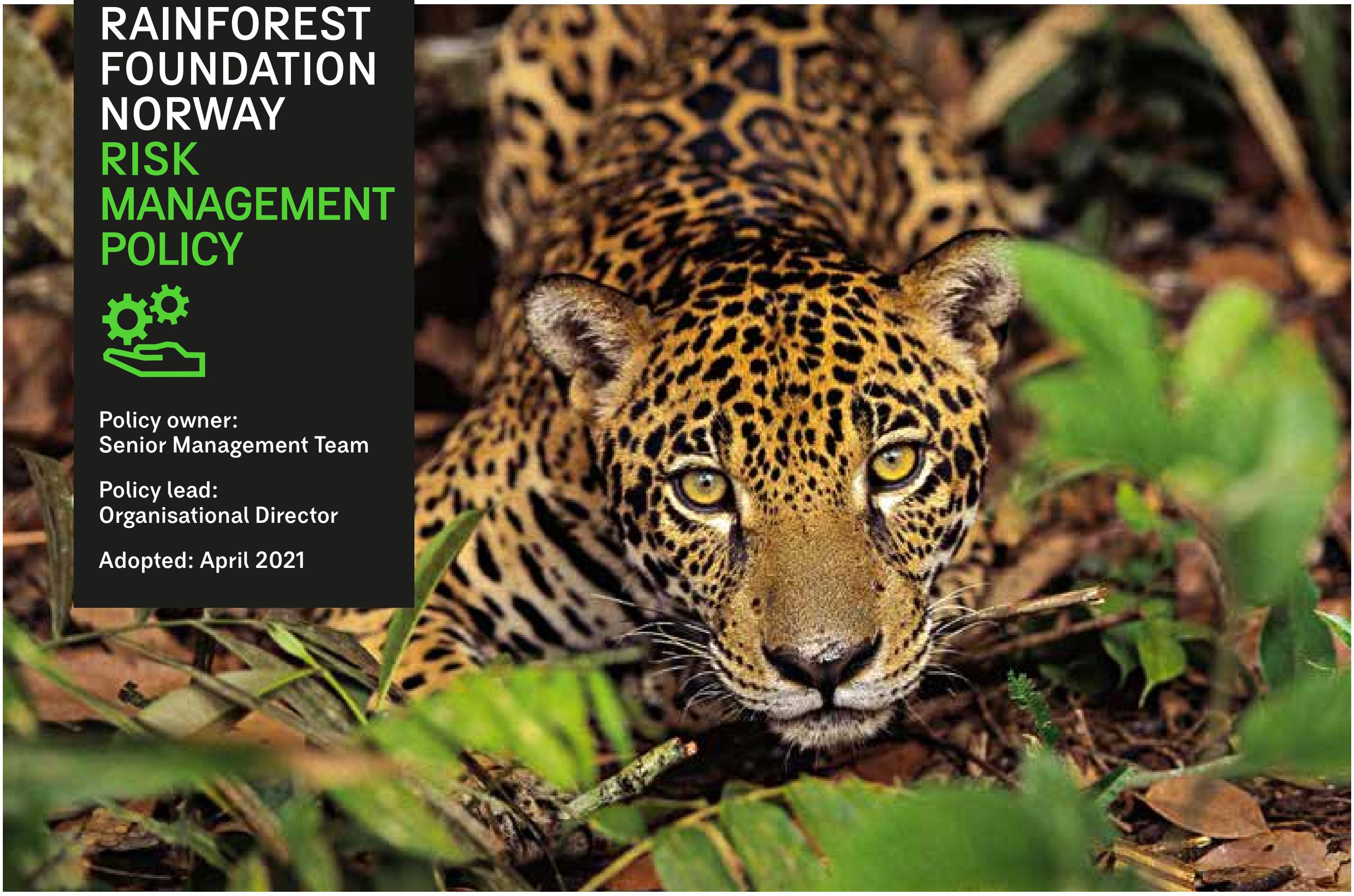


Photo: Araquém Alcântara

1. Purpose and scope of the policy

Risk management is an integral part of all organisations, whether public, private, or non-governmental. The purpose of the risk management policy is to provide guidance regarding the management of risk to support the achievement of our objectives, ensure the security of our staff and assets, ensure organisational, financial and operational sustainability and safeguard against our activities causing unintentional harm to others.

RFN works in high-risk countries and areas and with issues that are controversial and challenge vested interests. It is impossible to save the world's remaining rainforests and secure the rights for the peoples who live there without accepting risk. The risk to the world and humanity if rainforests are lost is probably infinitely higher. Managing risk is therefore not about avoiding risk, but to manage risk in such a way that we are likely to achieve our objectives, including avoiding harm to ourselves and others.

This policy applies to all working process in RFN. It forms part of RFNs governance framework and applies to all staff. RFN will actively work to increase partners' capacity in risk management and will consider this to be a requirement in the future.

While we cannot predict the future with certainty, risk management helps us identify the most critical uncertainties and act to minimize the probability and consequences of negative events. Risk management is part of RFN's endeavours to reduce the number of threats and improve the way we respond to them.

RFN and partners identify and handle risks in various ways, partly through specific tools for systematic risk management, partly implicitly in planning and implementation of activities. This policy lays out a structured risk management approach that will improve RFN's risk management by enabling:

- More risk factors being identified in an early stage of planning and implementation
- Better informed decisions on allocation of resources, taking risk into account
- More coherent approach to risk across the organisation, less subject to individual variations among staff and partners when it comes to their focus on risk
- Early and effective communication of and response to critical issues by relevant stakeholders, including donors
- More informed and more useful evaluations

In total: Fewer deviations and surprises, and higher likelihood of achieving desired results in line with strategic and organisational objectives.

2. What is risk?

RFN definition of risk:

"Risk is an uncertain event, that, if it occurs, will have a negative effect on objectives"

With "objectives" we mean not only programme/project objectives but also other objectives such as securing the reputation and financial sustainability of the organisation and core values such as staff safety. Keeping others safe from unintentional harm from our interventions is also a core objective and value.

This policy is focused only on negative effects of uncertainty, and with objectives we mean both specific intervention objectives (impact, outcomes, and outputs) and the broader objectives of the organisation. Interventions may have Unintended Negative Effects (UNE) on the environmental and social context in which they take place. This is outside the scope of this policy.

Risk is closely associated with uncertainty – regarding events which may or may not happen as well as uncertainties caused by ambiguity or a lack of information; and uncertainties about what will be the consequences if the event happens. The level of risk is the probability of an event times the consequences if it happens. Therefore, risk is calculated thus:

RISK (R) = PROBABILITY (P) * CONSEQUENCES (C)

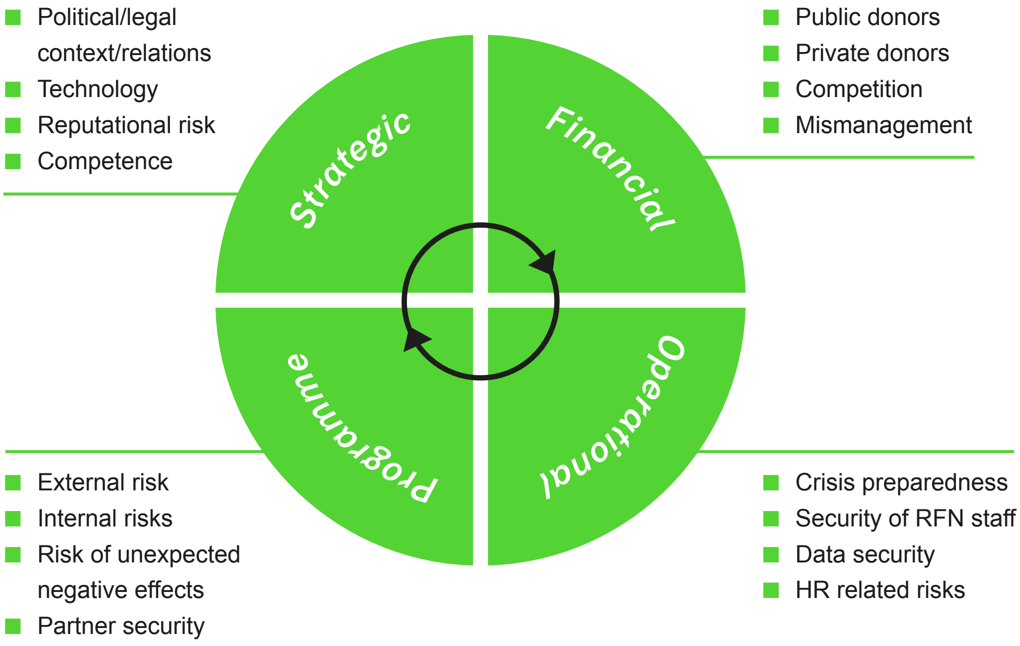
More precisely, we ask three questions:

1. What can go wrong?
2. How likely is it to go wrong?
3. If it does go wrong, what are the consequences?

The diagram next page shows how the different types of risk relate to each other. External risks may affect the intervention (programme/project), RFN and/or partners, and internal risks do the same. Unintended negative effects, however, are the effect of our interventions on the context in which we operate.

Photo: Kamikiá Kisêdjê

2.1 Main categories of risk



- Political/legal context/relations
- Technology
- Reputational risk
- Competence

- Public donors
- Private donors
- Competition
- Mismanagement

- External risk
- Internal risks
- Risk of unexpected negative effects
- Partner security

- Crisis preparedness
- Security of RFN staff
- Data security
- HR related risks

Strategic risks affect RFN as an organisation and are connected to external and internal sources of risk such as changes in the political and legal context in Norway, partner countries or internationally, technological developments, our reputation, and the competence of our staff. They must be considered when RFN makes long-term strategic choices, but they also sometimes require short-term tactical decisions. Responsibility for managing strategic risks rests with RFN Senior Management, with the Advocacy and Alliances Department having an important role on managing reputational risks.

Financial risks also affect RFN as an organisation and are usually connected to uncertainties regarding our main sources of income from institutional donors and private citizens in Norway, which are both competitive markets. Mismanagement of our funds is another risk in this category, but only gross mismanagement will affect RFN as an organisation. Responsibility for managing financial risks rests with the Finance Department and the Fundraising Department within their respective areas. The International Department has an important role in follow-up of financial mismanagement at partner/project level.

Operational risks are risks that affect our ability to carry out normal activities, and are often connected to security, either of RFN personnel, partner personnel or data. It may also be connected to broader human resource management issues, or even RFN's ability to continue operations in response to major crises affecting the organisation. Risk may be unintentional (e.g., accidents) or intentional (e.g., violence or data theft). Only the most serious risk events will affect the whole organisation. Overall responsibility for managing operational risks rests with the Organisation Department.

Programme risks have been separated from other operational risk because they specifically affect the ability to achieve programme/project objectives and/or the project/programme may have negative effects on stakeholders. Programme risks may have either internal or external sources, and RFN partners are part of the internal system as they implement most projects. Responsibility for managing programme risks rests with the International Department and the Advocacy and Alliances Department within their respective areas.

3. Guiding principles

The RFN risk management system is built on the following eight principles:[1]

1. **Integrated.** Management of strategic, financial, operational and programme risks shall be an integral part of all RFN activities. This includes projects implemented by partners.

2. **Structured and comprehensive.** RFN shall have a structured and comprehensive approach to risk management, based on this policy which shall be elaborated in guidance documents as needed. It shall encompass all relevant risks, and all parts of the organisation.

3. **Customised.** This policy with additional guidance documents, and its implementation, shall be customised and proportionate to RFN's internal and external context and RFN's objectives and resources.

4. **Inclusive.** Internal and external stakeholders shall be involved in an appropriate and timely manner in order to enable their knowledge, views and perceptions to be considered. RFN partners in rainforest countries are the most important external stakeholders to involve.

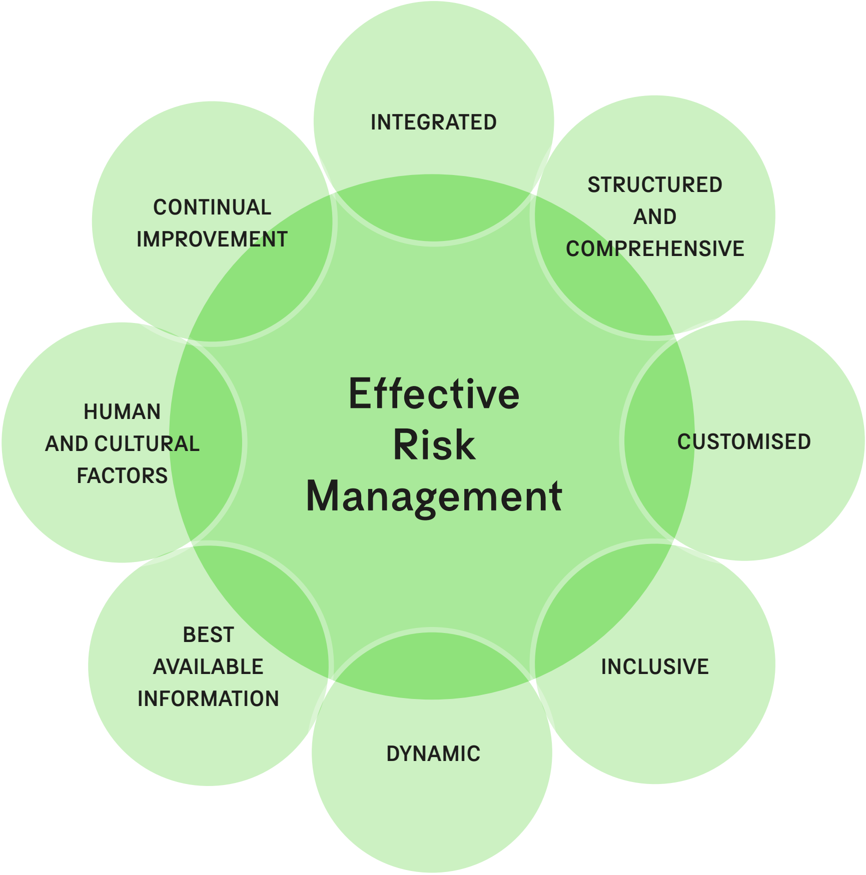
5. **Dynamic.** RFN's risk management shall anticipate, detect, acknowledge, and respond to changes in internal and external context in an appropriate and timely manner.

6. **Best available information.** RFN's risk management shall be based on historical and current information as well as future expectations, considering uncertainties and limitations associated with this. Information shall be timely, clear, and available to relevant stakeholders.

7. **Human and cultural factors.** RFN recognises that human behaviour and culture significantly influences all aspects of risk management and shall adapt this to the fact that we work in a multicultural context with large cultural differences.

8. **Continual improvement.** RFN is committed to continually improve its risk management through learning and experience.

These principles are the foundation for RFN risk management and are considered in the establishment of this policy and further guidance and process to be derived from it.


INTEGRATED
STRUCTURED AND COMPREHENSIVE
CUSTOMISED
INCLUSIVE
DYNAMIC
BEST AVAILABLE INFORMATION
HUMAN AND CULTURAL FACTORS
CONTINUAL IMPROVEMENT
Effective Risk Management

[1] The principles are taken and adapted from ISO 31000.

4. Leadership and commitment

4.1 Management by the senior management

Implementing the principles of risk management requires commitment from the RFN senior management – i.e., the Secretary-General and the Senior Management Team – through:

- Issuing and revising this policy on risk management.
- Ensuring that all components of this policy are operationalised and implemented.
- Ensuring that necessary resources are allocated to the implementation of this policy.
- Assigning authority, responsibility, and accountability at appropriate levels of RFN for the implementation of this policy.

4.2 Oversight from the board

The Board is responsible for overseeing risk management, and is required to:

- Approve this policy on risk management.
- Approve RFN's risk tolerance in the main areas of risk.
- Ensure that risks are adequately considered when approving RFN's strategies.

4.3 Integration – design – implementation – evaluation – improvement

Integrating risk management shall be customised to RFN's needs and culture and be part of RFN's governance, strategy, objectives, and operations. Everyone in RFN has responsibility for managing risk, and it is a dynamic and iterative process. Determining accountability and oversight roles for risk management are integral parts of RFN's governance.

The **design** of RFN's system for managing risk and UNE is based on an understanding of RFN's internal and external context and a clearly stated commitment by the top leadership and the Board to continual management of risks. It requires that authorities and responsibilities for relevant roles are assigned and communicated at all levels of RFN, and appropriate resources for risk management are allocated. It shall include an approach to consultation and communication which ensures that relevant information is collated, synthesised and shared, feedback provided, and improvements made.

Implementing the policy requires engagement and awareness of stakeholders, to ensure that risk management is a part of all RFN activities, including decision-making, and that changes in external and internal context is captured.

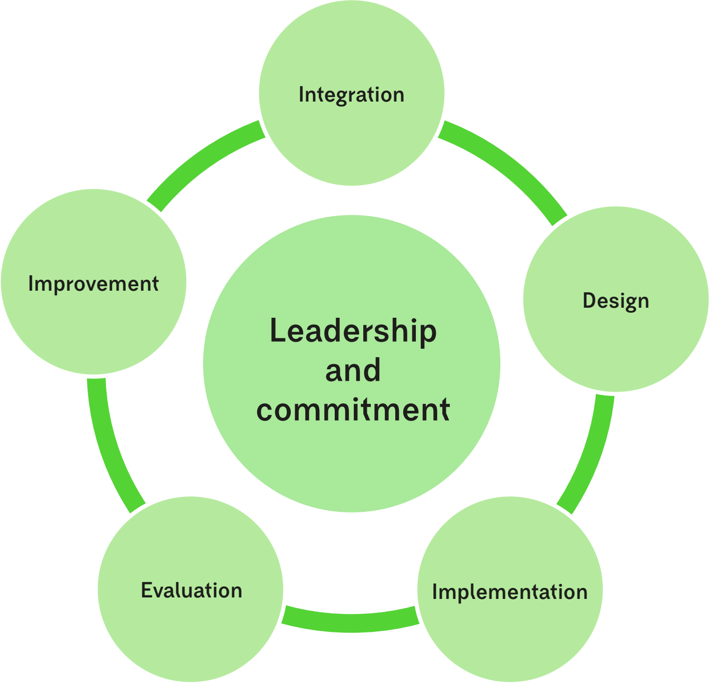
Evaluation of the effectiveness of RFN's risk management should take place periodically.

RFN shall continually monitor and adapt its risk management to address external and internal changes, to continually **improve** the suitability, adequacy, and effectiveness of this system. As gaps or improvement opportunities are identified, RFN shall plan to fill/exploit them.

4.4 Risk tolerance

Risk tolerance is the amount and type of risk that an organisation is prepared to pursue, retain, or take in pursuit of its objectives[2], including willingness to accept UNE. RFN must balance the potential benefits of its activities (for itself and for other actors) against potential damage to itself and other stakeholders triggered by risks connected to the same activities. Defining the risk tolerance encourages a consistent approach to risk throughout the organisation, although the risk tolerance will vary across risk categories.

The risk tolerance of RFN is to be broadly defined by the Board, for a limited number of areas, such as reputation, safety of staff, finance, partners, and intervention objectives. The risk tolerance should be reviewed regularly and based on clear criteria.



[2] Eric Marsden: «The ISO 31000 standard on risk management", risk-engineering.org

5. Risk management

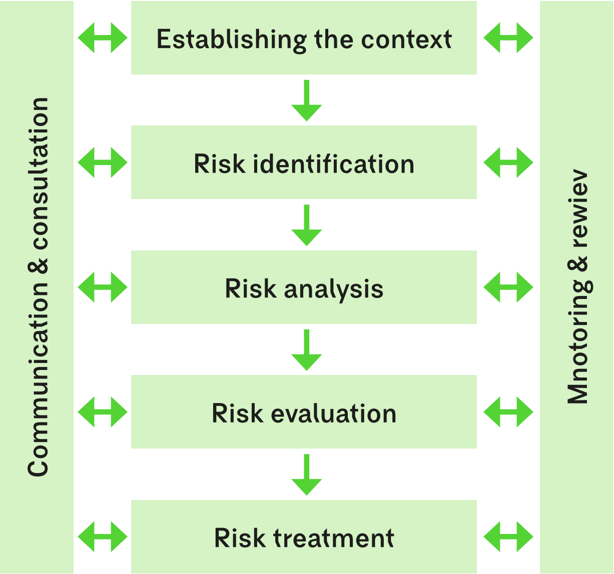
5.1 Understanding risk management

RFN definition of risk management:[3]

"Coordinated activities to direct and control an organisation with regard to risk."

The risk management process includes identifying, analysing, evaluating, and treating risks. The three first steps are commonly termed risk assessment. At all stages of the risk management process, monitoring & review, and communication & consultation, must be integrated, and prior to risk assessment, the context for the risk management be established.

THE ISO 31000 RISK MANAGEMENT PROCESS



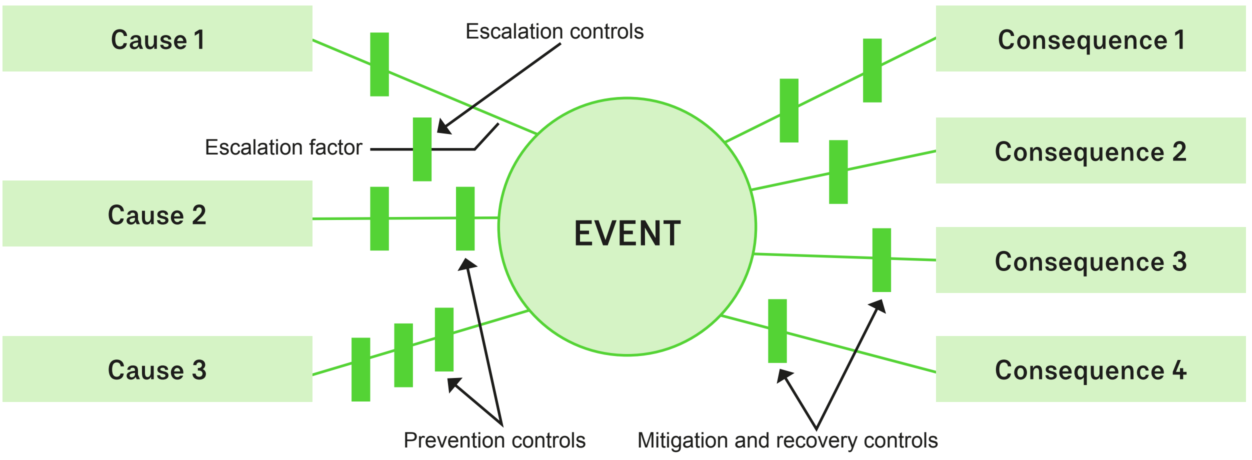
Source: Erik Marsden, risk-engineering.org

Risk Treatment can focus on reducing probability (P) or consequences (C) by introducing barriers to the causality before and/or after the risk event.

Photo: Thomas Marent

[3] Definition taken from ISO 31000.

EXAMPLE BOW-TIE DIAGRAM



Source: ISO/IEC 31010:2009

5.2 The risk management process

The risk management process involves the systematic application of policies, procedures, and practices to the activities of communicating and consulting, establishing the context, and assessing, treating, monitoring, recording, and reporting risk. Each of these parts of the process are outlined below.

5.2.1 Communication and consultation
Communication seeks to promote awareness and understanding of risk, whereas consultation involves obtaining feedback and information to support decision-making. It needs to take place throughout the risk management process. For RFN, communicating and consulting with our partners is of the utmost importance, as they have superior contextual knowledge about the environment they operate in, and they will be responsible for a large part of the risk treatment measures.

The framework for RFN's Stakeholder Communication Channel is described in section 6.3.

5.2.2 Establishing the scope, context and criteria
This involves defining the scope of the risk management process, understanding the internal and external context, and defining criteria for risk management. The purpose is to customise the process and enable effective and appropriate risk treatment.

Defining the scope is about defining which level (e.g., strategic, operational, project etc.) of the risk management process, including which organisational objectives are to be considered. Typical levels for RFN will be project, programme (often country), agreement (donor) and overall organisational level.

Defining the context is based on the defined scope and is about understanding the internal and external environment of the activities to which risk management is applied. This does of course depend on the scope (level) previously defined.

Defining risk criteria is about being clear about risk tolerance and defining criteria for risk evaluation (e.g., how levels of risk are determined and measured).

5.2.3 Risk assessment
This is the overall process of risk identification, risk analysis and risk evaluation.

5.2.3.1 Risk identification
The purpose is to find, recognise and describe risks. Risk identification is done throughout the organisational management and programme cycles, with special emphasis during planning phases. One advantage of early risk identification, besides enabling early response, is the identification of secondary/associated risks arising from already identified risks. Risk identification should therefore be one of the key topics to discuss with stakeholders, especially partners. It should be emphasised when planning activities and then revisited at relevant subsequent milestones. Normally, RFN partners will have the main role in identifying project level risks, in close dialogue with RFN, while RFN has the main role in identifying other types of risk.

Risk sources may be internal or external to the system that is the target of risk management. At project/programme level the "system" includes RFN and our (project implementation) partners; at other levels it usually just includes RFN.

5.2.3.2 Risk analysis

The purpose of risk analysis is to comprehend the nature of risks and their characteristics and assess the level of risk. An event can have multiple causes and consequences and affect multiple objectives. Risk analysis can be undertaken with varying degrees of detail and be qualitative, quantitative or a combination of the two. Risk analysis provides input to risk evaluation and insight for decisions on risk mitigation.

Responding to all risks with the same attention and in a similar manner would be counterproductive. Identified risks are therefore analysed to assess how much risk they present to objectives. This is done by assessing, for each risk factor, the probability of occurrence of the possible events that constitute the various risks, and the consequences of the events if they occur.

RFN does not intend to quantify risk levels by economic or other measures. RFN uses a standard ranking approach where probability and consequences are ranked on scales from 1 to 5, where 5 indicate the highest level of risk. Detailed scales for analysing risk are given in the risk management manual.

Based on this assessment of risk level and its two components, risk levels can be divided into five categories, from insignificant to extreme risk. The colours represent the urgency of risk response planning and determine reporting levels. For risks levels medium and higher, additional risk treatment will be necessary and for risk levels high/extreme, objectives must also be reconsidered if risk treatment cannot bring the risk level down to medium or lower.

5.2.3.3 Risk evaluation

The purpose of risk evaluation is to support decisions, comparing the risk analysis with established criteria to determine if action is needed.

The five types of decisions normally considered, for each risk, are:

1. Undertake further analysis before deciding
2. Do nothing
3. Maintain existing controls
4. Consider additional risk treatment options
5. Reconsider objectives

RISK EVALUATION MATRIX

IMPACT

LIKELIHOOD

	Negligible (1)	Minor (2)	Moderate (3)	Severe (4)	Critical (5)
Certain/ imminent (5)	Low risk	Medium risk	High risk	Extreme risk	Extreme risk
Highly likely (4)	Low risk	Medium risk	High risk	High risk	Extreme risk
Likely (3)	Insignificant risk	Low risk	Medium risk	High risk	High risk
Possible (2)	Insignificant risk	Low risk	Low risk	Medium risk	Medium risk
Unlikely (1)	Insignificant risk	Insignificant risk	Insignificant risk	Low risk	Low risk

Source: Norwegian Refugee Council

Photo: Araquém Alcântara

5.2.4 Risk treatment

The purpose of risk treatment is to select and implement options for addressing and reducing risk. It includes:

1. Formulating and selecting risk treatment options
2. Planning and implementing selected options
3. Assessing the effectiveness of implemented options
4. Deciding if the remaining risk is acceptable
5. If not, taking further treatment (repeating #1-#4)

5.2.4.1 Risk treatment options

Selecting risk treatment involves balancing our objectives against the costs of risk treatment and the potential costs of remaining risk. Treatment of risks is prioritised according to a mitigation hierarchy:

1. Avoiding risk
2. Where avoidance is not possible, reduce risk
3. Where the risk is not sufficiently reduced in advance, mitigate the residual consequences.
4. Where the residual risk is not sufficiently reduced, transfer/share the consequences
5. Any risk which is not treated in any of the above way, must be accepted or the activity must be reconsidered if residual risk is unacceptably high.

5.2.4.1.1 Avoiding risk

When risks can be anticipated they can be avoided by acting so the threat no longer can happen or no longer has a negative effect on objectives. This, in effect, severs the causal link between source and event, or between event and consequences. Avoidance may seem the answer to all risks but avoiding risks may also mean losing out on the potential gain that accepting the risk may have allowed.

5.2.4.1.2 Reducing risk

When avoidance in not possible, or the cost of avoiding outweigh the benefits, the risk can be reduced by acting in advance to reduce the probability of the risk event and/or the consequences if it occurs. This is the most common way of treating risks and the key is that by anticipating the risk we can act in advance to reduce probability and/or consequences.

5.2.4.1.3 Mitigating consequences

Where the risk is not sufficiently reduced in advance, the residual consequences when the risk has occurred may be further mitigated. These actions should also be pre-planned (contingency planning) but can only reduce the consequences, not the probability, as they take place after the risk event has occurred.

5.2.4.1.4 Transfer/share consequences

Where the residual risk is not sufficiently reduced, the consequences can also be transferred or shared, for example through contracts. Insurance is one type of risk transfer that uses contracts. Sharing is common in projects where both parties share the loss if the risk occurs and may be used between RFN and partners. Other times it may involve contract language that transfers a risk to another party without the payment of an insurance premium. Liability among contractors is very often transferred this way.

5.2.4.1.5 Accept residual risk

Here, the decision is made to accept the residual risk. All risks that are not avoided, reduced, mitigated or transferred are accepted by default. Risk acceptance is a viable strategy for small risks where the cost of reducing risk would be greater over time than the total losses sustained but also for risks that are so large or catastrophic that they either cannot be insured against, or the premiums would be infeasible (but where the probability is so low that you go ahead with the intervention anyway). If, however, the remaining risk is assessed to be unacceptably high, the activity must be reconsidered and possibly cancelled.

The categories are not mutually exclusive, and options should be selected in accordance with RFN objectives, risk tolerance and resources, and consulting with and considering the values, perceptions, and risk tolerance of our partners. Risk treatment may also introduce new risks that must be managed.

Risk treatment plans specify how chosen treatment options for each risk are to be implemented and monitored. The plans are integrated in RFN project cycle management and other plans and processes. The treatment plan for each risk will span from very brief (only a listing in the risk register) to comprehensive plans specified in much detail, with specific actions, time frame, designated responsibility and perhaps a budget. The plans shall be agreed between stakeholders (e.g., RFN and partners).

5.2.5 Monitoring & review

Monitoring and review of the risk management process is to be a planned part of the risk management process and take place in all stages of it. It will be incorporated throughout RFN management, monitoring and reporting activities.

Risks monitoring and review includes keeping track of already identified risks, reassessing risks, as well as identifying new risks and planning a response to these. This involves the continuous update of the risk register and risk treatment plans in an iterative process. In project management, this is most naturally done in connection with annual planning and reporting, which should always involve revisiting the risk register and risk treatment plan.

6. The system for managing risk

The system for managing risk is organisation-wide and integrated into the management systems of RFN. The main components of the risk management system are:

1. Identification, analysis, and evaluation of potential risks.
2. Treatment of risks.
3. Effective community/stakeholder engagement and communication, including adequate complaints and feedback mechanisms.
4. Monitoring, review, learning and improvement of the system for managing risk
5. Emergency Preparedness and Response
6. Development of capacity of RFN and partner organisations regarding points 1-5 above.

6.1 Identification, analysis and evaluation of risks

Risks are to be identified, analysed, and evaluated during the proposal and planning stage of every intervention implemented by RFN and/or partners and every strategic decision made by the organisation. This is a compulsory due diligence exercise.

Identified, analysed, and evaluated risks are to be recorded in the Risk Register for the intervention. The Risk Register has one section for risks against achievement of objectives and one for unexpected negative effects on cross-cutting issues, but they are assessed using the same methodology.

Based on the screening and the risks identified, the intervention/decision is categorised a low, medium, or high risk for not achieving objectives, and low, medium, or high risk for unexpected negative effects on crosscutting issues.

- For low-risk interventions, the risk register will be the main tool for risk management.
- For medium risk projects, there may be a need for additional analysis and risk assessment
- For high-risk interventions, there will be a need for additional analysis and risk assessment, and a requirement to reconsider objectives and modalities, including cancellation.

For individual risks, those evaluated as medium, high, or extreme will require risk treatment measures. For those evaluated as low or insignificant risk, such measures are optional.

6.2 Treatment of risks

The Risk Register is the main tool for managing treatment of risks, including reporting on this. The Risk Register is updated every year as part of the Annual Planning process, or more frequently if internal or external circumstances cause significant changes to the threat picture. New risks may be added, and outdated risks deleted from the Risk Register, and risk analysis, evaluation and treatment measures may change.

Treatment of risks is prioritised according to a mitigation hierarchy given in section 5.2.4.1.

The Risk Register is also the main basis for reporting, but such reporting must also include risks that have materialised without being foreseen and therefore not included in the Risk Register. Reporting on risks is the responsibility of the partner organisation if the intervention is implemented by them.

Responsibilities for monitoring risk (risk owner) and implementing treatment measures (risk assignee) is to be specified for each risk and each treatment measure and entered in the Risk Register.

6.3 Stakeholder communication channels including complaints and feedback mechanism

RFN stakeholder communication channels serve many purposes. They build stakeholder trust and confidence, promote organisational learning in RFN and among partners, and provide early warning signals when risks materialise. The channels must be legitimate, accessible, predictable, equitable, transparent, rights-compatible, and sources of continuous learning and based on engagement and dialogue. The communication channels build on existing measures and procedures and are integrated with stakeholder communication which is not directly related to risks. They serve three primary functions:

- Stakeholder engagement to identify potential risks, assess them and develop optimal treatment measures.
- External complaints and feedback mechanisms ensure that feedback, concerns, and complaints are received in a safe and culturally and technologically appropriate way; dealt with in a timely, fair, impartial, confidential, and respectful way; and that decisions and actions are communicated to the concerned parties with due regard for transparency and privacy.
- Feedback to complainant and reporting to affected communities, not only on complaints mentioned above, but all issues related to risks.

There will be stakeholder communication channels and complaints and feedback mechanisms run by RFN and applicable to all interventions. For medium and high-risk interventions there may be additional intervention-specific channels/mechanisms. RFN also strives to ensure that its partner organisations have their own, contextually, and culturally appropriate, channels and mechanisms, and will support them in developing such mechanisms when needed. Division of responsibility between RFN and partners must be clearly spelt out in contracts.

6.4 Monitoring, review, learning, and improvement

Risk management is to be monitored through the regular administrative and project management systems of RFN and partners. The SMT and relevant Departments determine how this is done for each of the main categories of risk (see section 2.1).

Data from reports, reviews and evaluations shall be used by relevant teams in RFN for learning and improvement purposes. Intervention-level risk data shall feed into corresponding analyses at country level and feed into the strategy and programme process. The Organisation Department (Strategy and Results Team) shall facilitate cross-team and cross-departmental learning and improvement and support partner capacity development in this field.

For programme risks, the Annual Plan and Annual Report are the two most important mechanisms. For larger, multi-year interventions, risks should also be integrated in the Terms of Reference for external evaluations unless these are narrowly focused on issues where risks are not relevant.

6.5 Emergency preparedness and response

RFN must be prepared to handle unforeseen emergencies both in our programmes and for the organisation as such. Emergencies come in many guises and may be connected to the different areas of risk, such as safety of staff, finances, reputation, partner organisations, political context and, unexpected negative effects on others. One cannot prepare for every emergency, but one can prepare for the most critical types of emergencies by developing contingency plans for the most important scenarios.

Based on previous experience and current analysis or risks, RFN will develop a limited number of contingency plans for the most important emergency scenarios and inform and train staff in their implementation (see capacity development below).

6.6 Capacity development

The abovementioned systems require development of capacity in RFN and partners, both before implementing the new system and continuously as it is being used. Capacity development must be tailor-made for the roles and responsibilities outlined above and focus on the practical skills required to make the system work.

Photo: Ronny Hansen/RFN

7. Operationalisation

This policy is operationalised through manuals, guidelines, and tools to be developed and continuously updated and improved. This policy takes effect when it is has been approved by the RFN Board.

ATTACHMENT 1:

THE RFN RISK MANAGEMENT FRAMEWORK

The risk management framework is based on the scope/ purpose, risk tolerance and risk management process described above.

The main responsibility for managing risks and reporting to the Board on risk management rests with the RFN Secretary-General supported by the Senior Management Team. The management, of specific categories of risk, however, is delegated further, with the main division of responsibility being:

- The Senior Management Team is responsible for managing strategic risks
- The Organisation Director is responsible for managing operational risks and the Finance Director is responsible for managing financial risks, with the Advocacy and Alliances Department having an important role in managing reputational risks.
- The International Director and the Advocacy and Alliances Director are responsible for managing programme risks within their respective areas.

More detailed division of responsibility for managing different categories of risk is given in the table next page. All risks are to be registered in appropriate Risk Registers. Formats for Risk Registers will be developed by those responsible for them. The Risk Registers will be the main tool for managing, treating, monitoring, reviewing risks and communicating and consulting about risks.

DIVISION OF RESPONSIBILITIES

The effectiveness of management of risks depends on their integration into the management systems of RFN. It includes aspects such as integrating, designing, implementing, evaluating and improving such management, and it requires leadership, commitment and a culture of safeguarding against risks. Management of risks is therefore integrated as a cross-cutting methodology applied to all significant processes in the organisation, be it management of programmes, finance, fundraising, human resources, communications etc. It is a unique exercise for each organizational process.

There shall be a focal point for risk management in the RFN secretariat. The focal point is placed in the Organisation Department and is responsible for providing technical support to the rest of the organisation and maintaining risk management systems and tools.

The advisers in the International Department must also be able to support the RFN partners in their work in this area. Capacity development of partner organisations is the responsibility of Country Teams in the International Department, supported by the Organisational Department. The Organisational Department (Strategy and Results team) will develop training modules and materials, and the Country Teams will be responsible for training partners, assisted by the Organisational Department or the Finance Department when required.

DIVISION OF RESPONSIBILITIES

Unit / position	Responsibility	Policies, procedures and other key documents and tools
Board	Approve risk policy and approve RFN's risk tolerance in the main areas of risk. Ensure that risks are considered when setting objectives for RFN.	Key Performance Indicators to include risk at a higher level (TBD) Risk tolerance summary (TBD)
Secretary General	Issue and revise the risk policy. Communicate the policy to all staff and prioritise and fund implementation of the corresponding management systems. Develop RFN's risk tolerance in the main areas of risk. Promote a culture of management of risks. Lead management of strategic risks in the SMT. Be accountable for implementation of this policy vis-à-vis external stakeholders and the RFN Board.	RFN Risk Management policy Risk register for strategic risks (TBD) Risk reporting routines to Board (TBD) Key Performance Indicators to include risk at a higher level (TBD)
Senior Management Team	Ensure procedures to comply with the policy are made and implemented in their departments and foster a culture where risks are assessed and controlled. Management of strategic risks and defining RFN's risk tolerance in various areas. Ensure that complaints are dealt with in accordance with regulations and procedures and concerned parties receive timely and adequate responses. Ensure resources to enable implementation of this policy. Implementation of risk management at programme and project level.	RFN Risk Management policy Risk reporting routines to SMT (TBD) Risk tolerance summary (TBD) & risk register for strategic risks (TBD) RFN Anti-Corruption policy RFN Protection from Sexual Exploitation, Abuse and Harassment policy RFN Annual Budget Departmental roll-out plans (TBD)
International Department	Ensure partners comply with the policy and build their capacity to assess and control risks. Cooperate with partners on reporting on risk management and project and programme level.	Roll-out plan for Int. Dept. (TBD) Programme risk management manual (TBD) Training materials for partners (TBD) Multi-year Plan, Annual Plan, Annual Report & Mid-year Report Risk registers (for project and country programme framework) RFN Anti-Corruption policy Procedures for handling of suspected financial irregularities
Organisation Department	Implementation of operational risk management: • Crisis preparedness • Security of RFN personnel • HR related risk • Data Security (GDPR etc)	Roll-out plan for Org. Dept. (TBD) Risk registers for operational risk (TBD) Risk, security, and precautionary measures RFN Anti-Corruption policy RFN Protection from Sexual Exploitation, Abuse and Harassment policy
Finance Department	Implementation of financial risk management: • Financial mismanagement, incl. fraud and corruption • Financial sustainability	Roll-out plan for Finance Dept. (TBD) Risk registers for financial risk (TBD) RFN Anti-Corruption policy Procedures for handling of suspected financial irregularities

DIVISION OF RESPONSIBILITIES

Unit / position	Responsibility	Policies, procedures and other key documents and tools
Advocacy and Alliances Department	In consultation with other departments, ensure that RFN has procedures to anticipate, manage and communicate issues that may pose reputational risks to the organisation vis-à-vis external stakeholders. Ensure that all RFN communications and social media accounts adhere to risk management standards to avoid risks to the security of staff and partners. Implementation of risk management for all global level activities including policy engagement, investor relations, and campaigns.	Roll-out plan for Advocacy and Alliances (TBD) Risk register for reputational risks (TBD) Risk register for global programme/ framework
Team Leaders	Ensure that risk management is carried out according to policies and procedures, and review and approve the recommendations of Programme Advisers. Ensure documentation of and learning from risk management, including those stemming from the complaints and feedback mechanism. Ensure that project/programme level complaints and feedback mechanisms work and that complains are forwarded according to rules and regulations.	Relevant risk registers Relevant roll-out plans (TBD) Programme risk management manual (TBD) Training materials for partners (TBD) RFN Anti-Corruption policy RFN Protection from Sexual Exploitation, Abuse and Harassment policy Procedures for handling of suspected financial irregularities
Strategy and Results team	Develop and improve frameworks and tools for risk management at project and programme level. Perform quality control of risk assessment, control and reporting at these levels. Support other departments in their implementation of the policy and be a knowledge and learning hub for risk management. Recruit external expertise to conduct specialised assessments and put in place specific mitigation procedures when required.	Risk register template (TBD) Training materials for staff (TBD) Training materials for partners (TBD)
Security Group	Emergencies concerning staff safety and security.	Risk, security, and precautionary measures Security rules, procedures and contingency plans

Rainforest Foundation Norway supports indigenous peoples and traditional populations of the world's rainforests in their efforts to protect their environment and secure their customary rights. RFN was established in 1989 and works with local environmental, indigenous and human rights organisations in the main rainforest countries in the Amazon region, Central Africa, Southeast Asia, and Oceania. RFN is an independent organisation, and part of the international Rainforest Foundation network, with sister organisations in the United Kingdom and the USA.

Rainforest Foundation
Norway

Rainforest Foundation Norway, Mariboes gate 8, 0183 Oslo Norway

rainforest.no/en