


Norwegian Ministry of Foreign Affairs



Review of Risk Management in the EEA & Norway Grants 2009-14

Oslo, 23rd December 2011

 **ERNST & YOUNG**

This report is only for the internal use of the Norwegian Ministry of Foreign Affairs for the purpose in which it was intended, and shall not be distributed to third parties without the express, prior, written consent of Ernst & Young. The report is intended as a summary of our work. Ernst & Young takes responsibility only for the contents of the report. Our liability remains as agreed in the terms of the engagement letter.

Acknowledgements

The Norwegian Ministry of Foreign Affairs has requested a review of Risk Management in the European Economic Area & Norway Grants 2009-14. The review has been carried out by Ernst & Young.

The project team includes professionals with experience of risk management, internal controls and knowledge of grant management and government administration. The involved team members from Ernst & Young have not conducted any prior work related to the European Economic Area and Norway grants or the financial mechanisms.

The report has greatly benefited from the contributions and comments from stakeholders in the European Economic Area and Norway Grants, including the Financial Mechanism Office, the Norwegian Ministry of Foreign Affairs, the Norwegian Association of Local and Regional Authorities, Innovation Norway, Climate and Pollution Agency and The Norwegian Association of Local and Regional Authorities.

The draft report has been reviewed by the Norwegian Ministry of Foreign Affairs.

The project team from Ernst & Young is responsible for the findings and recommendations in the report. The views and opinions expressed in the report do not necessarily correspond with the Norwegian Ministry of Foreign Affairs.

Sincerely,

Terje Klepp
Partner

Oslo, 23rd December 2011

Contents

	Page
Acknowledgements	2
Executive Summary	4
1. Introduction	6
1.1 Background	6
1.2 Objectives and scope	6
1.3 Approach and methodology	7
1.4 Hypothesis and audit criteria	8
1.5 Limitations	9
1.6 Schedule	9
2. Review of established framework for risk management in FM 2009-14	10
2.1 Corporate governance in public sector	10
2.2 Risk management framework	11
2.3 Observations, findings and recommendations	14
2.3.1 Strategy and policy	16
2.3.2 Roles and responsibilities	21
2.3.3 Routines and methodology	24
2.3.4 Reporting and monitoring	27
2.3.5 Competence and capacity	32
2.3.6 Tools	32
3. Identification and analysis of risks in the donor side management of the EEA & Norway Grants	33
3.1 Overview of identified risks and measures	33
4. Recommendations	38
4.1 Prioritized recommendations	38
4.2 Next steps	39
Appendices	47
A – Maturity charts	47
B – The link between performance management and risk management	53
C – Abbreviations and definitions	54

Executive Summary

The European Economic Area and Norway financial mechanism were established in 2004, in connection with the historic enlargement of the European Union and European Economic Area in 2004. The grants are administered by the Financial Mechanism Office in Brussel. The Financial Mechanism Office reports to the Financial Mechanism Committee and to the Norwegian Ministry of Foreign Affairs. The FMO is responsible for the day-to-day running of the two grant schemes and serves as a contact point. The FMO cooperates with the National Focal Points in the beneficiary states.

The grants are specifically targeted at lowering social and economic inequalities in the European Economic Area, and strengthen bilateral relations with the beneficiary countries.

Objectives and scope of the project

The objective of the project is to strengthen the risk management framework of the EEA financial mechanism. The assessment of the risk management framework cover four key areas: structure, people, processes and systems. Within these areas we have assessed several important elements that are necessary to include in an acceptable risk management framework. The work has been conducted by a team from Ernst & Young.

Approach and methodology

The project is based on independent, objective assessments and suggestions of improvement related to 1) the established framework for risk management and 2) assistance to identify potential risks in the donor side management. We have conducted desk top studies of the established risk management framework including document reviews and interviews with key personnel affiliated with the grant schemes. Identification of potential risks have been done in collaboration with NMFA and FMO.

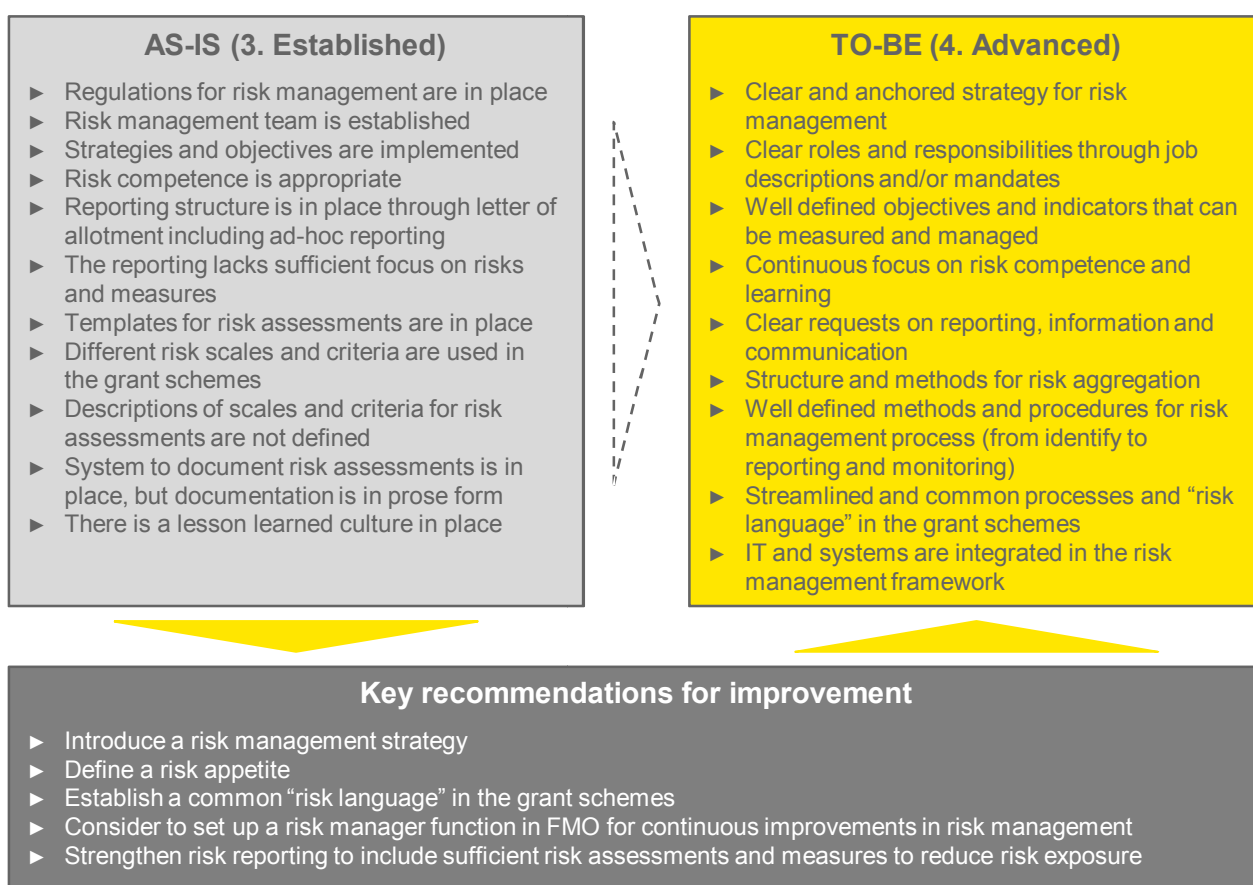
We have used a maturity model for assessment of the risk management framework with scores from 1 - 5. Based on the maturity of the evaluation criteria we have suggested improvements to close gaps between leading practice and the as-is situation. Recommendations are based with the intention of taking the next step on the risk management maturity model (from 3. Established to 4. Advanced).

Executive Summary

Key findings and recommendations

Review of established framework for risk management in FM 2009-14

The figure summarizes our assessment of the risk management framework.



Identification and analysis of risks in the donor side management of the EEA & Norway Grants

We have identified potential risks in the risk management and on the donor side management of the grants. These are presented with critical success factors and measures in section 3. However, we have listed the top five risks below.

#	Top five risks
1	"Risk language" – risk assessment scales and criteria
2	Competence in risk management
3	Cultural differences between involved people and organizations
4	Quality of data and information
5	Irregularities and potential corruption

1. Introduction

1.1 Background

The European Economic Area (EEA) Grants represent a contribution of approximately 990 MEUR by Norway, Iceland and Liechtenstein and are awarded to 15 Beneficiary States in Central and Southern Europe. Norway is responsible for approximately 95 % of the total funding. The objective of the grant scheme is to reduce social and economical disparities between countries in the EEA and to strengthen the bilateral relations between the donor and Beneficiary States. The Norway Grants, funded solely by Norway, awards grants to the 12 newest EU member states. The Norway Grants has made available approximately 800 MEUR.

The Financial Mechanism Committee (FMC) has the decision-making authority regarding the EEA Grants. The Norwegian Ministry of Foreign Affairs (NMFA) has the decision-making authority regarding the Norway Grants.

The EEA & Norway Grants is administered and managed by the Financial Mechanism Office (FMO). FMO is a secretariat to the donor countries in their management of the grants. The office is responsible for the administration of the EEA & Norway Grants 2004-09 and EEA & Norway Grants 2009-14, with the former in the process of being concluded.

In 2008 Norad conducted an assessment of the EEA & Norway Grants 2004-09. An important recommendation from the report is to do program- and country specific risk assessments and identify risk reducing measures. The NMFA has decided to review the established risk management for FM 2009-14, and to identify risks related to the donor side management of the EEA & Norway Grants.

1.2 Objectives and scope

The objective of the project is to strengthen the risk management framework of the EEA financial mechanism.

This is realized by independent, objective assessments and suggestions of improvements related to 1) the established framework for risk management and 2) assistance to identify potential risks in the donor side management.

1. Introduction

1.3 Approach and methodology

The project consists of the following phases: *Planning, Execution and Reporting*.

The project has been conducted with the following approach:

- ▶ *Hypothesis* and *audit criteria* based on information from the initial meeting and review of documentation and leading practices.
- ▶ *Review of documentation* which includes an assessment of processes, routines, guidelines, procedures, standards, rules and regulations.
- ▶ *Interviews* and *workshops* with key personnel.
- ▶ *Documentation* of project activities, interviews and workshops.
- ▶ *Report* with observations and review of risks and suggested improvements.

The project consists of two parts:

Part 1 – Review of established framework for risk management in FM 2009-2014

A maturity analysis of the established framework for risk management has been developed based on the criteria listed above. This has provided a good indication of which (potential) areas should be improved, and prioritized with recommendations.

Part 2 – Identification and analysis of potential risks in the donor management of the EEA & Norway Grants

This has resulted in a risk map of the donor side management which highlights identified risks. An action plan has also been presented with identified measures to reduce the risk exposure.

1. Introduction

1.4 Hypothesis and audit criteria

Hypothesis

Part 1

- ▶ An appropriate framework for risk management in the grant management scheme is established.
- ▶ The risk management is concentrated towards the achievement of the objectives of the EEA & Norway Grants.
- ▶ The risk management ensures and highlights risks and variations between different programs and countries.

Part 2

- ▶ Critical success factors are identified and documented for management and control.
- ▶ Risk assessments of the donor side management are performed.
- ▶ Risk reducing measures are identified for the donor side management.

Audit criteria

- ▶ Ernst & Young's framework for leading risk management (based on the COSO-model).
- ▶ Norwegian Government financial regulations – chapter 6 Management of grant schemes.
- ▶ Grant regulations.
- ▶ Guidelines and standards for EEA & Norway Grants.

1. Introduction

1.5 Limitations

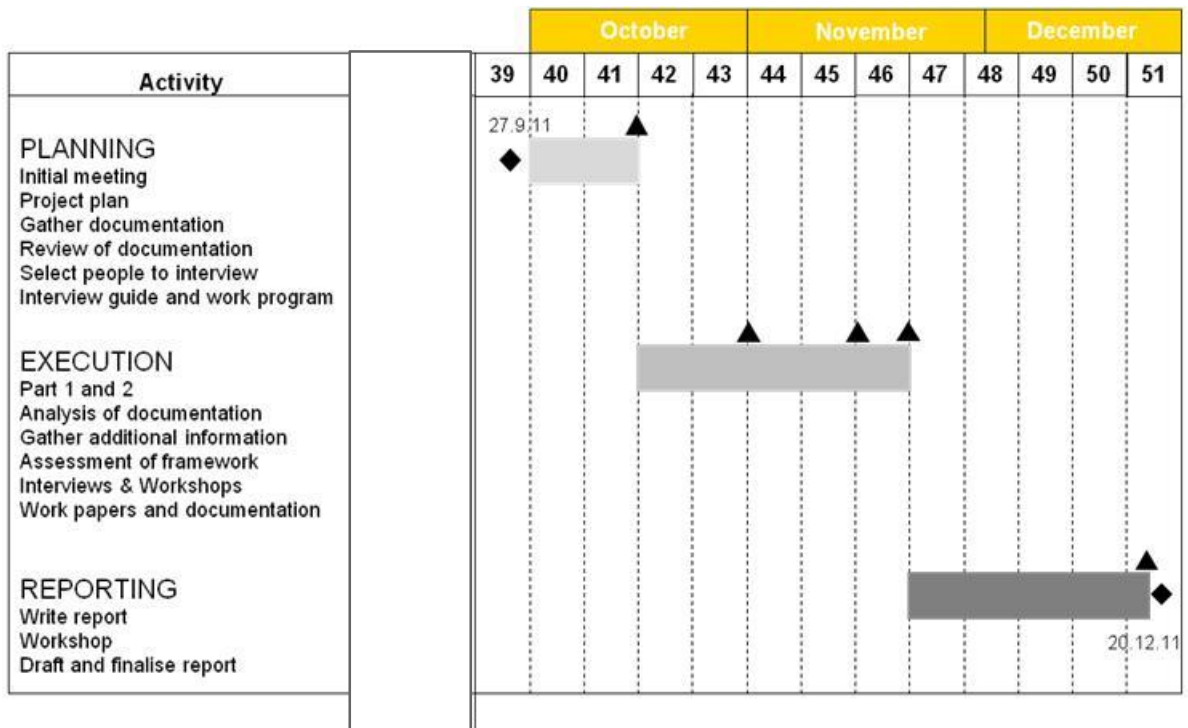
The project has covered those areas of the grants management and responsibilities which FMC, FMO and the NMFA performs. Other responsibilities and procedures are not included in the project.

The project is based on review and analysis of documentation received, interviews with key personnel and workshops. We have focused on established frameworks, routines and processes to evaluate whether these are appropriate compared to leading practices.

The project has not tested the employee's compliance of established framework, routines and processes. The project does not cover an assessment of the quality in commenced risk management activities. In addition, the project has not covered implementation of suggested improvements or new methods, routines and processes.

1.6 Schedule

The project has been planned and carried out within the timeframe outlined in the plan of progress/activities below. The project period has been from September to December 2011.



2. Review of established framework for risk management in FM 2009-14

All organizations face uncertainty, and the challenge for management is to determine how much risk it will accept in order to create maximum value for their stakeholders. Risk management is necessary to ensure that the organization's objectives are reached.

Risks are undesirable events or circumstances that can lead to failure of reaching an organization's goals and objectives. Risk management processes are implemented in the organization in order to continuously identify risks, evaluate them and consider how risks should be managed, mitigated, monitored and reported.

Appropriate risk management helps the organization to better achieve its objectives through a continually better overview of the organization's risks, and what risks that require measures to ensure maximum value. The purpose is to create a strong control environment where continuous risk assessments, active information and communication, and monitoring activities are part of the processes.

2.1 Corporate governance in the public sector

In this section we briefly describes how risk management is related to the organization's corporate governance structure.

Organizations in the public sector are given guidance from higher authorities through the governance dialog. The management's mission is to provide objectives and performance requirements for the operational level in the organizations. This is done through strategy, preparation of operational plans, allotment letters and budget, as well as active management, internal and external dialogue and monitoring. Management anchoring and competent resources are crucial for achieving strong corporate governance in the organization.

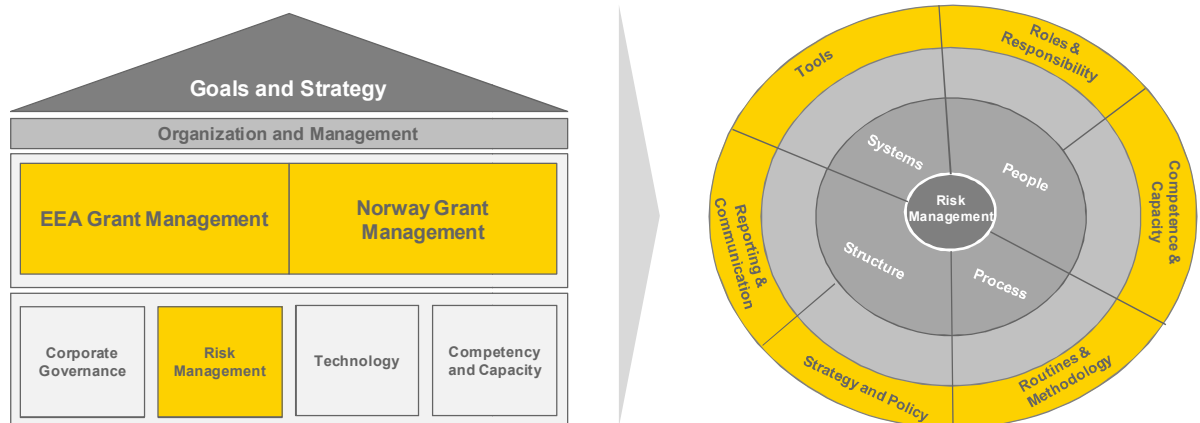


2. Review of established framework for risk management in FM 2009-14

In the public regulations, performance management is the guiding principle which also require appropriate risk management and internal controls. This means that the objectives and performance requirements are specified by key performance indicators in the planning phase, and followed up by monitoring and reporting. Similarly, risks should be identified, assessed and prioritized during the planning phase, and followed up by monitoring and reporting. This ensures that the organization has integrated the performance and risk management in the corporate governance process, as the figure on the previous page shows.

2.2 Risk management framework

The figures below show the mapping and analysis dimension of the project. We distinguish between structure, people, process and systems that together ensure a comprehensive and structured approach to assess the established framework for risk management.



The figure on the left side illustrates enablers that support FMO in achieving its objectives and strategy. The level of ambition and purpose is expressed and defined through the stated objectives and strategies. These will be achieved through an appropriate organizational structure and management model, and by focusing on the appropriate processes and operations. Finally, the organization has several measures in form of management principles, systems and technology, competence and capacity to contribute to effective and appropriate processes and achievements.

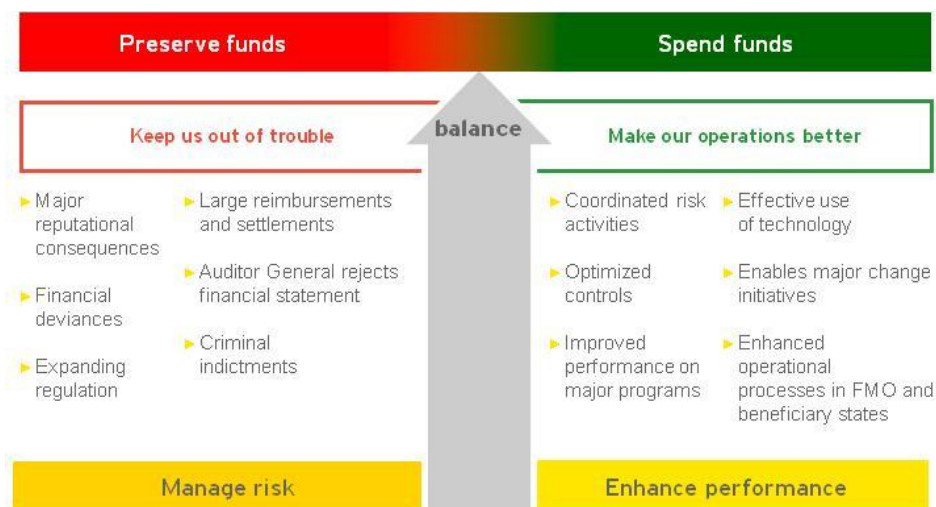
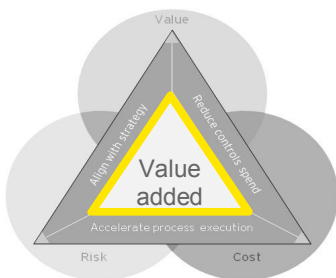
In this project we have opted to assess a range of key areas within structure, people, process and systems. These are presented in the figure to the right above and are described more in detail in the maturity model in appendix A. The key areas are analyzed in section 2.3 Observations, findings and recommendations.

2. Review of established framework for risk management in FM 2009-14

We have used a maturity model to assess the key areas presented on the previous page. A maturity model is an effective tool to illustrate and analyze the gap between current and recommended level of risk management. The used maturity model has two dimensions – current situation and recommended practice. NMFA's ambition level with regard to risk management have not been defined in this project. Therefore, the recommended state is based on Ernst & Young's risk management expertise and leading practice. We have developed several maturity profiles of selected key areas which have been aggregated for an overall assessment of the established risk management framework. These profiles provide a picture of the current situation, and is a tool to identify areas for improvement and thereby to strengthen the current risk management.

To assess the maturity of the current risk management, we have used a scale from 1 to 5, where 1 is basic and 5 represent leading practice. For areas where the cost of effective risk management is considered excessively high, or it is so extensive that it retards the performance management of the funds, 4 can be seen as the recommended state.

There is a challenge to strike the right balance between risk management and performance management. It is important to have the right balance between risk, cost and value. In this project the focus will nevertheless be on the risk dimension. The figure below shows the relationship between managing risk and enhance performance.



2. Review of established framework for risk management in FM 2009-14

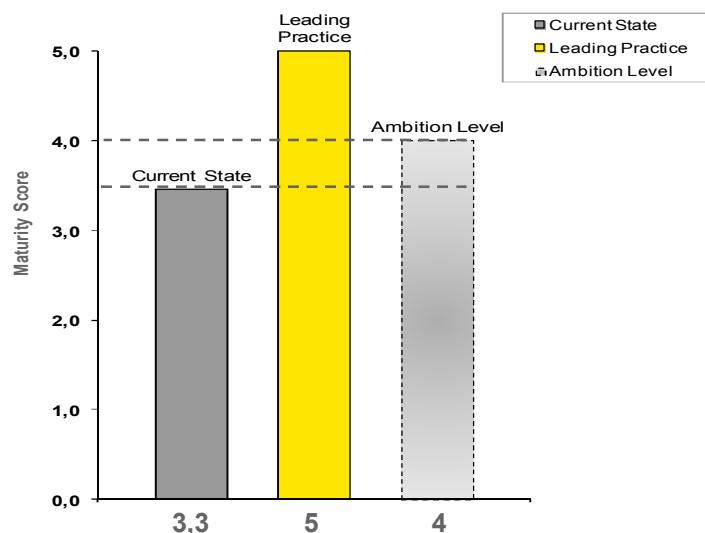
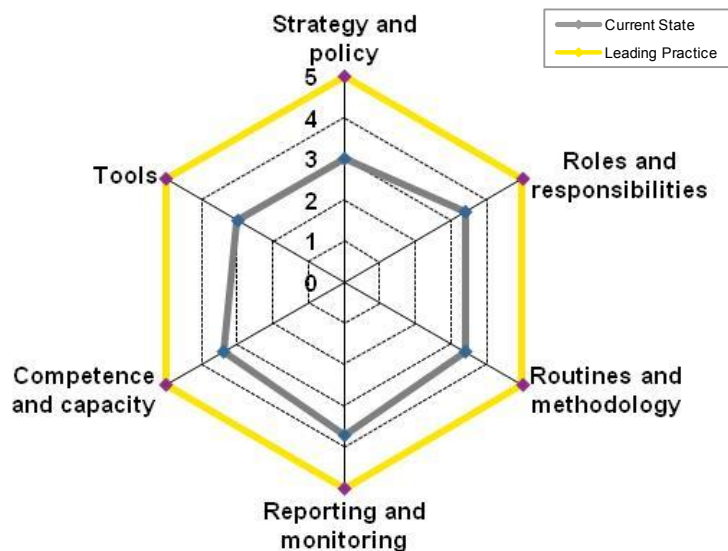
It is essential that the organization conduct its activities with performance in mind. It is also important that it is aware of the risks facing it as a whole and the objectives it is striving to achieve. EEA & Norway Grants use result based management, which is a form of performance management, to operate and measure the outcome of the funds' activities. Result based management has risk management elements built in. Too much performance focus may lead to unexpected, unwanted surprises, while too much focus on risk management may retard performance and progress in the programs' objectives.

One experience from the mid-term evaluation of FM 2004-09 was too much focus on control at the expense of performance and progress of the projects. In FM 2009-14 there has been a change in organizational design and procedures to ensure coherence between the results framework and adequate reporting on results. The figure on the previous page shows the paradox of finding the balance between results and control, which is inherent in any grant management scheme.

2. Review of established framework for risk management in FM 2009-14

2.3 Observations, findings and recommendations

The figures below show the identified maturity profiles and key areas and the aggregate maturity profile of current risk management.



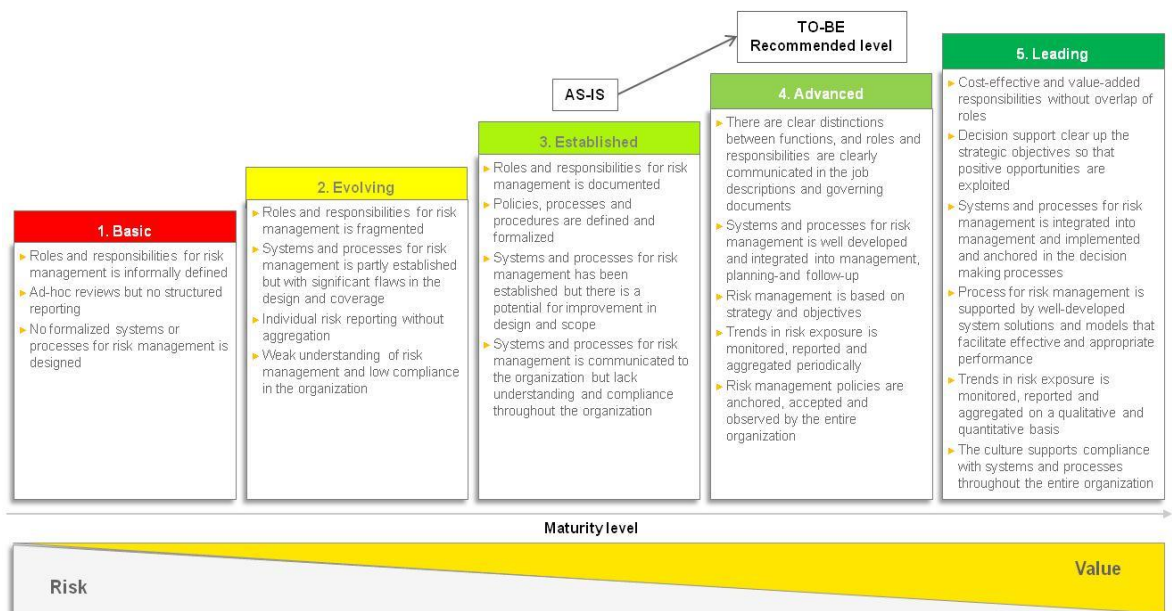
The leading practice level of the risk management is not linked with the ambition level of FMO or the Donor States. The stippled pillar is only intended to illustrate that the current state should be assessed against NMFA's hypothetical ambition level, in order to identify the true gap and thereby necessary measures to strengthen the risk management function.

2. Review of established framework for risk management in FM 2009-14

As the aggregated maturity model shows, the risk management is at a acceptable level (3. Established) as shown in the figure below. However, we recommend to further improve the established risk management framework towards leading practice. This is due to the substantial amounts of grants, potential risks for irregularities, the importance of the grants too succeed as well as public and media focus on the grants.

The first step should be to develop an advanced system for risk management, as shown in the figure below (4. Advanced). This is done by introducing a common risk management framework. Our recommendations for reducing the gaps in the current risk management framework, and improve it to the advanced level, are presented subsequently with our observations and findings in this report. We have also summarized and prioritized all of our recommendations in section 4.

The figure below shows the overall maturity model criteria's and scores which we have used as basis for our assessment. The right level of risk management needs to be defined by the donor states and FMO, taking the balance between risk, cost and value into consideration.



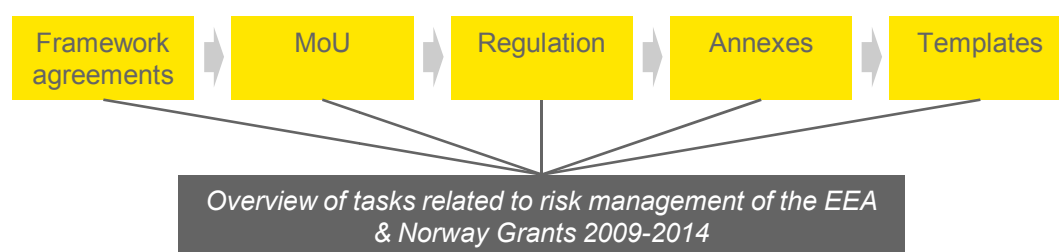
In the following we present more detailed descriptions of the key areas that we have analyzed in the maturity model framework.

2. Review of established framework for risk management in FM 2009-14

2.3.1 Strategy and policy

Management documents and strategy

"*Overview of tasks related to risk management of the EEA & Norway Grants 2009-2014*", chapter 2, states that there is no separate risk management strategy, and that the risk management activities are embedded in the general management of the funds. This makes the risk management activities an integrated part of the management of the funds. However, it makes it challenging to update, review and improve the risk management activities. The document is only an overview of the risk management activities in the grants processes. It does not describe the overall risk strategy or policy. It is, however, useful in explaining the interrelation between the relevant risk management documents, as illustrated below.



There are several references in the above mentioned document to the *Regulation*, which have references to annexes, which again have references to other documents. This makes it challenging to use, review and maintain the documents. The documents have a hierarchical structure, but this is not immediately intuitive for the diverse group of intended readers. This poses challenges as to which documents are agenda setting, and which documents are supporting whom.

The structure and contents of the "*Overview of tasks related to risk management of the EEA & Norway Grants 2009-2014*" is still work in progress, and it is a natural source for a defined risk management strategy. The document's content is formalized, communicated and consistently deployed across the organization. The document is reviewed on a continuous basis, as it is still under development.

2. Review of established framework for risk management in FM 2009-14

Recommendations

1. A clear and extensive strategy document for risk management should be introduced. The strategy document could include the following:

EEA & Norway grants risk management strategy	
<ol style="list-style-type: none"> 1. Introduction <ul style="list-style-type: none"> - Purpose and objective of the manual - Document hierarchy 2. Document administration <ul style="list-style-type: none"> - Document administration responsibilities 3. Roles and responsibilities <ul style="list-style-type: none"> - FMC - NMFA - Risk department - Head of risk - Managing director - Legal advisor - Internal audit - Compliance 4. Risk overview <ul style="list-style-type: none"> - Definitions - General policy statements - Risk appetite - Internal controls - Information technology - Human resources - Risk management framework 	<ol style="list-style-type: none"> 5. Risk identification <ul style="list-style-type: none"> - Risk identification - Identifying new risk areas 6. Risk assessment <ul style="list-style-type: none"> - Risk assessment overview - Cause and effect categories 7. Risk measurement <ul style="list-style-type: none"> - General policy statements - Risk measurement overview - Evaluation criteria and model 8. Risk monitoring <ul style="list-style-type: none"> - Risk management and monitoring guidelines 9. Risk reporting <ul style="list-style-type: none"> - Key risk indicators - Status reports on trends in risks and mitigating actions 10. Periodic meetings <ul style="list-style-type: none"> - General policy statements - Weekly management meetings - Monthly management meetings - Committee meetings

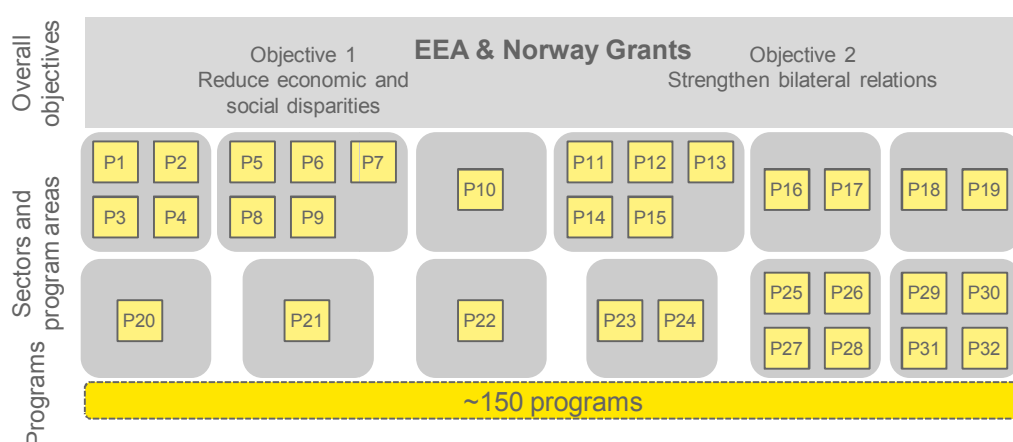
2. There could be a need to develop a document hierarchy, as shown below, to improve information and communication and ensure a common “risk language”. This could be part of the strategy document.



2. Review of established framework for risk management in FM 2009-14

Objectives and key performance indicators

Based on the grants' objectives and strategy, specific targets are defined and translated into a set of objectives and key performance indicators (KPI). A KPI is defined as a measure that an organization use to gauge or compare performance in terms of meeting their strategic and operational goals. The objectives and KPIs build upon relevant and well-defined drivers. The figure below shows the structure of the objectives and measurements hierarchy.



Two overall objectives are defined for the EEA and Norway Grants, broken down to one objective for each of the 32 program areas, a total of 160 outcomes for the 32 program areas, and (at least) 2 outputs per program outcome. The FMO has defined approximately 400 indicators for the 160 outcomes, and the Program Operators are advised to choose one or a few robust indicators. 400 indicators is a number which is reaching the upper limit of what we find possible to aggregate on a manageable level on the program area and grants level.

Efficient risk management requires clearly stated objectives and KPIs in order to identify and follow-up potential risks that can threaten the organizations and grants achievements. FMO will identify a limited number of outcome indicators (10-15) which will be measured and reported on systematically by the FMO. Each program will also have the number of indicators considered necessary and sufficient for the Program Operator to report to their stakeholders.

One of the two overall objectives, "Improve bilateral relations", is an objective which is challenging to measure. This makes it correspondingly challenging to define related outputs and outcomes. The ones currently in use are clearly related, although the measurement still seems challenging. NMFA has hired a third party consultant to review and improve these measures, an initiative which is appropriate. Further elaboration of the issue is therefore scoped out of this project.

2. Review of established framework for risk management in FM 2009-14

High number of indicators makes it challenging to apply them consistently across all projects and programs considering the number of different people and organizations involved. The aggregation of indicators on the defined objectives for each of the 32 program areas is not defined in the governing documentation. Indicators and measures are defined for the program outcomes and outputs, but these numerous many and probably too detailed to aggregate on an overall level.

The purpose of any objective must be to fulfill them, and hence, to measure indicators of success. The challenges related to measure fulfillment of objectives will by default lead to challenges in measuring risk of not fulfilling objectives.

Recommendations

3. We support FMO's work on reducing the number of indicators and focus more on an appropriate number of critical indicators that need to be fulfilled to reach the objectives related to projects, programs, sectors and the overall level. We would like to point out that it is important to ensure linkages between the individual countries' priorities and the grants' objectives and KPIs.

Risk appetite and risk limits

Risk appetite is the amount and type of risk an organization is willing to accept in pursuit of its objectives. Risk limit thresholds are established to monitor that actual risk exposure does not deviate too much from the risk target and stays within an organization's risk tolerance/risk appetite. Exceeding risk limits will typically act as a trigger for management action. Without a clear risk appetite it is difficult to design an efficient risk management function.

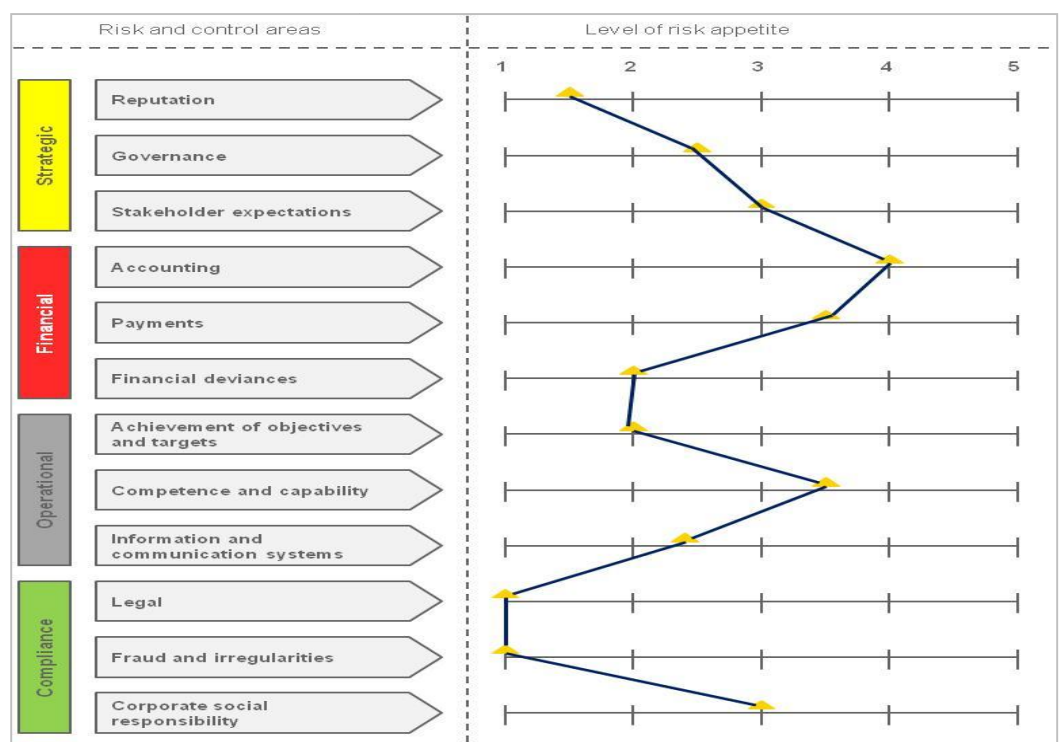
Except for fraud and corruption, risk appetite and risk limits are not defined on any level. Meanwhile FMC and NMFA implicitly accepts high risk on certain programs and projects, due to political considerations. The risk appetite for fraud and corruption is defined as zero. This is based on a decision by Stortinget that there is a non-tolerance for fraud and corruption in the grants schemes. This is practiced today through strong principles for follow-up and monitoring of financial deviances, which is resource-demanding. It is highly unlikely to achieve zero financial deviances in practice given the amount of funds, transactions, people and organizations from different countries and institutions involved.

We are also informed that payments in advance are practiced for the EEA & Norway Grants in the period 2009-14. The previous period (2004-09) practiced arrear payments. This is an example of an increase in the risk appetite.

2. Review of established framework for risk management in FM 2009-14

Recommendations

4. A risk appetite with associated risk limits should be defined and documented in the suggested strategy document. Below we have shown an example on how to determine a risk appetite with qualitative statements. The score 1 means zero-tolerance and strong control while a score 5 suggests a higher risk appetite and acceptance of larger deviances and faults.



The initial step in the development of risk appetite statements is gaining an understanding of what risk appetite defines and how it can be integrated within the current governance structure, strategic direction, operational targets, financial planning and compliance framework. The next step is to formalize the risk management framework and develop risk appetite statements. The organization draws up critical and important risk statements and gives them a score from 1 to 5 dependent on the risk willingness.

A clearly understood and articulated statement of risk appetite helps unlock value by better aligning decision making and risk management in the organization. This helps the organization focus on key areas for achieving the objectives and better balance risk, cost and value.

2. Review of established framework for risk management in FM 2009-14

2.3.2 Roles and Responsibilities

Established roles and responsibilities for risk management

Risk management is integrated into the performance management of the EEA & Norway Grants. This secures a lean performance of risk management activities. However, the absence of an organizational chart, where risk management activities, roles and responsibilities are clear, pose a risk as to whether the current risk management activities and capacity is sufficient or too comprehensive. This can potentially lead to unknown/undesired risks being taken, or that risk management is conducted at the unnecessary cost of performance.

Certifying authority in beneficiary states (i.e. Ministry of Finance) are defined as being ultimate responsible for any mismanagement of the funds. This works as an efficient and effective outsourcing of financial and compliance risk from the donor states and the FMO. It also gives incentives to conduct risk management on the beneficiary state level as the latter is obliged to reimburse mismanaged funds. However, this might lead to excessive control by the beneficiary states.

Donor program partners assist the program operator in the risk assessments conducted during the program proposal and annual reporting by the program operator. The donor program partner also reports on risks within relevant programs to the FMO in the annual progress report.

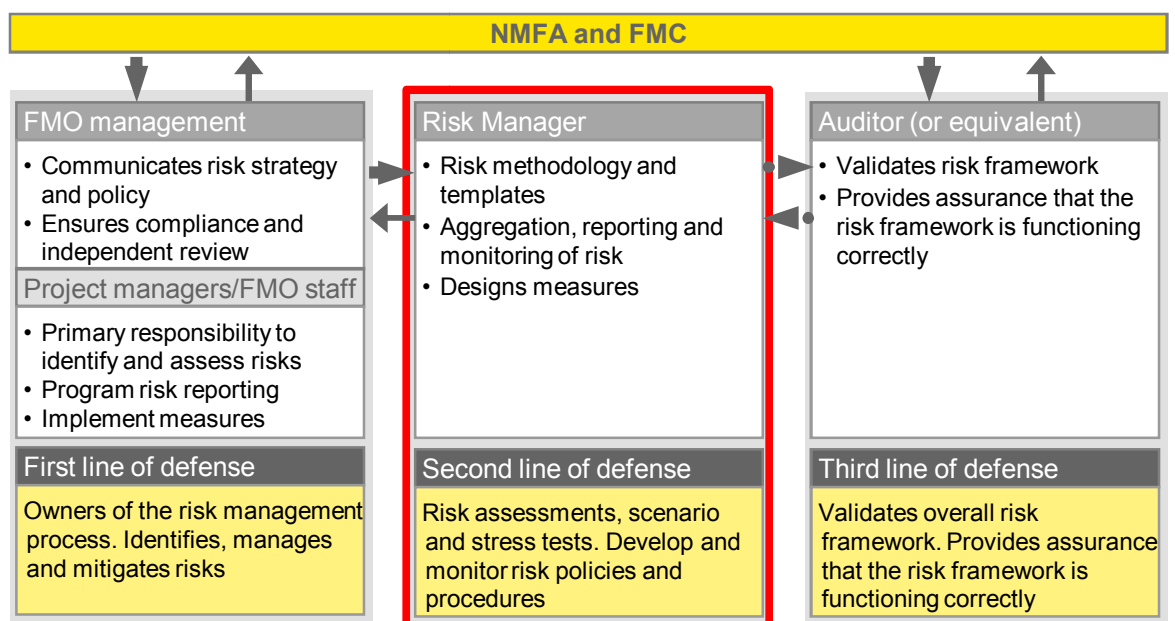
Roles, activities and responsibilities regarding risk management are aligned between the NMFA, FMC, FMO, beneficiary states, and program and project levels.

A risk management team is established in FMO. This is appropriate from a risk management perspective. There are however, some weaknesses in the current setup. The team does not have a clear mandate. Risk management activities are not adequately addressed or detailed in the team members' job descriptions. The roles and responsibilities of the risk management team is not clearly communicated within the FMO, nor to external people or organization. The high number of projects and programs will require substantial capacity and competence in risk management, especially with regard to the aggregation, reporting and monitoring of risks. These employees, in the risk management team, already work full time on other assignments, and it is a risk that they might not have capacity, nor the core competences, to undertake thorough risk management activities.

2. Review of established framework for risk management in FM 2009-14

Recommendations

5. The current risk management team is an ad-hoc function with no defined mandate, and the members' job descriptions have limited risk management responsibilities. A description of the risk management team's roles and responsibilities needs to be established. This should be documented in the suggested strategy document for risk management in the FMO.
6. In order to achieve a high maturity level of risk management it is common practice to have a risk manager, constituting an organization's "second line of defense". This is an important role as shown below. The absence of this role can be imagined by removing the red box, which is where FMO is today. The current risk management team does not fulfill the role, since their primary focus is on assignments to support the performance of the grants, and thus have a clear role in the "first line of defense".

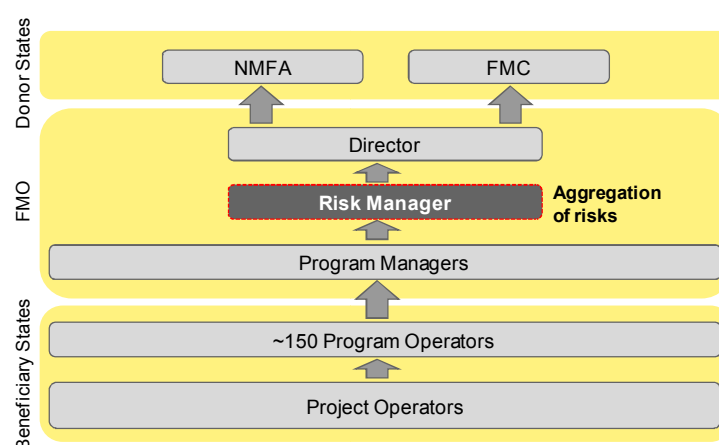


Establishment of a risk manager function with a dedicated responsibility to aggregate, report and monitor risks on each program area should be considered. This should be done since there are objectives defined on each of them, which needs to be followed-up and measured. The risk manager should also be responsible for designing appropriate procedures and guidelines for performing risk management (Identify – Assess – Manage – Report – Monitor – Compliance).

2. Review of established framework for risk management in FM 2009-14

Recommendations (cont.)

6. The risk manager, with a clear mandate and job description, ensures appropriate responsibility for managing, developing and maintaining risk management methodology and reporting to the Director, which again reports results and risks further to FMC and NMFA. The risk manager should develop and distribute a common methodology to all stakeholders involved in risk management. This will ensure uniform reporting of risks throughout the entire reporting chain, using sound and uniform methodology. He/she can provide guidance and suggest improvements to other personnel involved in risk management, especially the program operators. The risk manager's role in FMO's risk reporting chain is shown below.



Job descriptions and Delegation of Authority

On November 1st 2011 FMO conducted a reorganization. Job descriptions for Deputy Director, Head of Finance, Head of Sector and Head of Country have been finalized. At the release of this report job descriptions for other positions are being revised. Moreover, risk management responsibilities that are described are limited to "oversee risk management activities". The documents are not specific as to what this responsibility includes. Neither are there any descriptions of risk management responsibilities for the Director and Deputy Director. The ultimate responsibility for risk management in FMO rests with the Director, and it is her/him that should be formally responsible for reporting this to NMFA and FMC.

Recommendations

7. Risk management should formally be on the Director and Deputy Director's agenda, and hence, in their job description. All employees should have a job description specified for their position and roles. The job descriptions should also contain risk management responsibilities, where applicable.

2. Review of established framework for risk management in FM 2009-14

2.3.3 Routines and methodology

Description of routines and procedures for risk management

According to the regulation, risk management activities are conducted on several points in the value chain, such as in the application, appraisal, management and evaluation part of the programs. These are mentioned both where the responsibilities of the various personnel involved, as well as where the different stages in the processes are explained. The activities are limited to risk assessments, but with little explanation of exactly how these should be conducted. This leaves room for different interpretations and methodology, which will affect the usefulness of the output of the risk assessments.

Transparency International (TI) is developing a methodology for risk assessment to identify and prioritize fraud and irregularity risks in the beneficiary states. The agreement with TI does not explicitly state that it is an assessment related to fraud or corruption, although given the institution involved, such issues will be paramount. A potential risk in the project is that Transparency International uses other definitions, scales and methodology in their assessments than the other involved people and organizations. This could make the aggregation and prioritizing of identified risks challenging.

Several templates are in use across the grants scheme. However, these do not have common risk definitions, categories or scales. The risk scale in use throughout the EEA & Norway Grants is limited to High – Medium – Low, but there is no elaboration as to what these definitions include nor the difference between them. There is a risk that the applicants have diverging interpretations of what high, medium and low probability and impact means. A manageable aggregation is therefore challenging to do by the program operators and FMO. It also poses a risk as to whether the aggregation of risks from different projects and programs will end up with a correct risk profile for all the grants. The design of measures can therefore be misguided, spending resources on the “wrong” risks.

Templates and tools are owned by the risk management team, but “risk language” is still under development and implementation is in progress. An evaluation scale is defined in the “Monitoring Guide for Program Operators”, but it needs to be improved.

2. Review of established framework for risk management in FM 2009-14

Recommendations

- Clear and documented scales and criteria for risk assessments should be introduced for all the people and organizations in the EEA & Norway Grants. This will contribute to a common “risk language” and help the organization to better prioritize the most critical risks and manage resources more efficiently. An example of a risk criteria model is given below.

It is also important to make sure that people and organizations in the EEA & Norway Grants have the same understanding of critical risks. A common procedure with guidelines and communication of these needs to be carried out.

Value	Rating	Probability	Description
5	Most likely	> 90 %	The risk will certainly occur more than once within the next 1-3 years
4	Likely	60-90 %	The risk will almost certainly occur once within the next 1-3 years
3	Moderate	30-60 %	The risk may occur at least once within the next 1-3 years
2	Seldom	10-30 %	The risk will rarely occur the next 1-3 years
1	Not likely	> 10 %	The risk is not likely to occur once within the next 1-3 years

Value	Impact area	Rating	Effect	Description
5	Reputation, economy, employees, management, society, customers, political leadership, external stakeholders etc..	Critical	> 200 MNOK	The national media storm Public distrust of the organization Longer downtime on mission-critical infrastructure Critical project fails Deviation from the budget of > 20 %, > 200 MNOK
4	Reputation, economy, employees, management, society, customers, political leadership, external stakeholders etc..	High	≤ 200 MNOK	Considerable criticism in national media, significant influence on achievements of objectives in several areas, significant disruption to infrastructure, deviations from the budget > 10 % < 20 %, ≤ 200 MNOK.
3	Reputation, economy, employees, management, customers, political leadership	Moderate	≤ 100 MNOK	Increased public awareness irregular service Significant project deviations (time / quality / budget), ≤ 100 MNOK
2	Economy, organization	Low	< 50 MNOK	No significant effect on the ability to achieve its goals, < 50 MNOK
1	Organization	Minor	< 20 MNOK	Insignificant effect, < 20 MNOK

The document “Monitoring Guide for Program Operators” is methodically sound, except that the probability scale should be quantified like the impact scale. The methodology could be distributed to all involved people and organizations that are responsible for conducting risk management activities in the grants scheme, both in the beneficiary states, FMO and in NMFA. The methodology and scale should replace the Low – Medium – High scale, as it gives more value, is easier to aggregate across projects and beneficiary states, and includes descriptions on the different criteria. This should be done in all templates currently in use to increase quality and uniformity of the risk assessments being done.

2. Review of established framework for risk management in FM 2009-14

Risk assessments of applications and distribution of grants

Risk assessments of applications are conducted by the program managers in FMO and the description of this process is under development by the risk management team. Risk assessments are conducted for all the applications and distribution of grants based on FMO employees' knowledge of associated inherent risks in risk categories.

Any applicant is obliged to conduct risk assessments on the program proposals submitted to the program operators. This includes a risk assessment section in the program proposal template. The template includes no guidelines on definitions nor how to use the scale provided (High – Medium – Low). The templates' measure plans have limited content related to how the risks are to be followed up by a responsible person, and do not provide specific deadlines. The same goes for guidelines on how to use the templates.

Recommendations

See recommendation number 7 and 8.

9. The risk assessment templates should include measure plans with measure descriptions, responsible persons, deadlines for implementation and follow-up schedule with status orientation.

Categorization and aggregation of risks

Risks are categorized on the project, program and beneficiary state level, but not formally aggregated on the program area or EEA & Norway Grants level. The risk aggregation seems to be incomplete as there are no formalized routines in place to measure, or aggregate, the risks of not achieving the objectives which are defined on the program area level. FMC and NMFA has indicated that they want risks to be reported on the beneficiary state level. In theory any objective is there to be fulfilled. The degree of fulfillment must be measured and reported. Risks of not fulfilling the objectives must be reported to give an overview of the overall risks, which is valuable information to the management of the grants when considering mitigating measures.

Recommendations

10. Establish guidelines and structure for risk aggregation, which should be a part of the strategy document for risk management.

2. Review of established framework for risk management in FM 2009-14

2.3.4 Reporting and monitoring

Management agenda

Risk management is increasingly on the agenda in management meetings and team meetings. The topic is also addressed in FMC and NMFA meetings.

However, risk management is only briefly mentioned in FMO management's job descriptions, and absent in the Director's job description. The establishment of a risk management team in FMO is evidence of the topic's increasing place on the agenda.

Risk reporting system

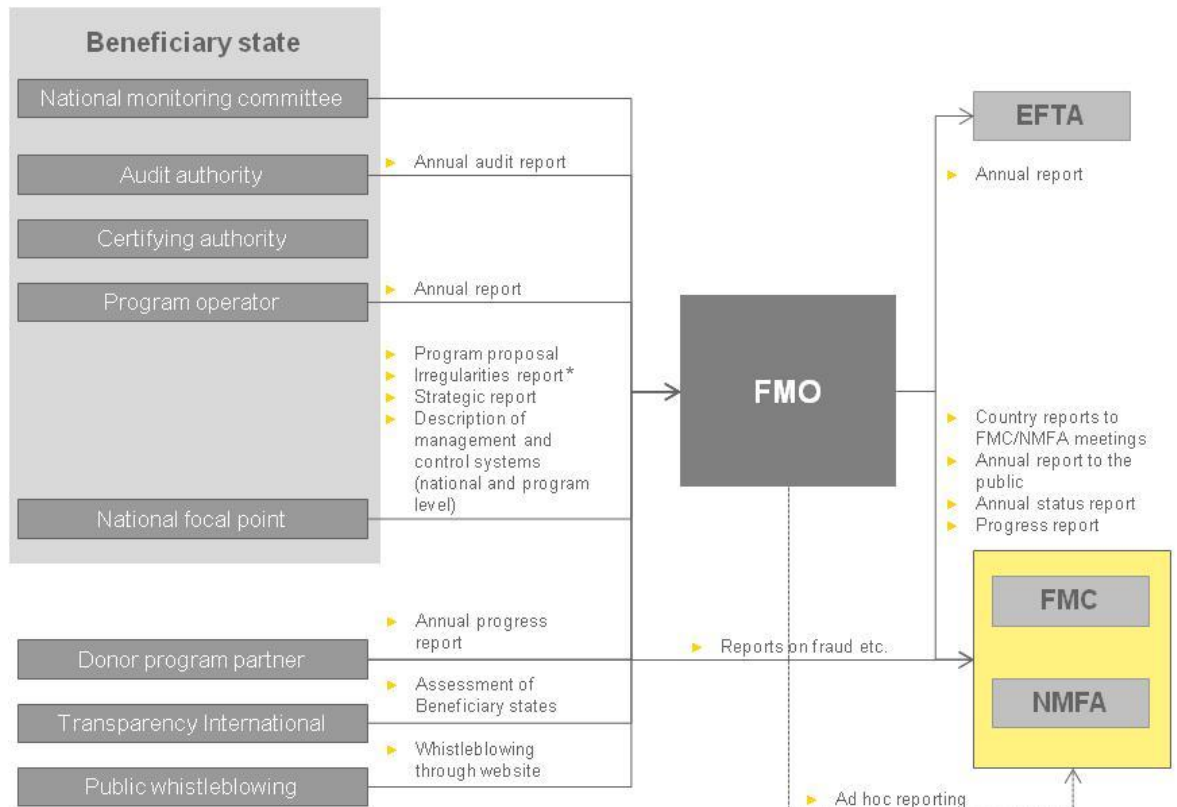
Reporting on risks are conducted on all levels in the grants scheme. Project operators report to the program operator which, in addition to the National focal point (NFP), reports to FMO in annual and strategic reports. There is also interim reporting of irregularities to FMO. However, there is no systematic aggregated reporting of risks on the program area level and sector level. This poses a challenge for FMO management's ability to have clear visibility on performance and risks on an aggregated level, and on the risks for not achieving the overall objectives.

There is a considerable inherent risk in the reporting chain, meaning that key messages in the risk assessments can be distorted in the exchanges between project operators, program operators, NFP, FMO and NMFA. As mentioned elsewhere in this report, a common use of definitions and scales are essential to mitigate this risk. The main reporting system DoRIS, currently does not remedy the issue as risk assessments in the system are only done in a prose form. For example are no risk maps that could visualize the risk assessment produced in the system.

On the next page we have shown the major elements (what is reported and to whom) in the established reporting scheme. The figure is not exhaustive as it relates to reporting lines and the number of reports that are prepared during a year or period in the grant scheme. For example, reports on irregularities may come from other than just the National focal point, reports from FMC and NMFA and statistical reporting in DoRIS are not included, and the Embassies are not taken into account.

2. Review of established framework for risk management in FM 2009-14

The figure below shows an overview of risk reporting where a beneficiary state is the program operator:



* A national public entity (NPE) is responsible for the preparation and submission of irregularities reports. In many beneficiary states this is a function taken on by the National Focal Point, but this is not always the case

Recommendations

11. The risk assessment sections in DoRIS should include scales for probability and impact of the risks. Alternatively, excel models can be used to ensure a common risk assessment and use of criteria instead of prose form.

2. Review of established framework for risk management in FM 2009-14

Risk management information

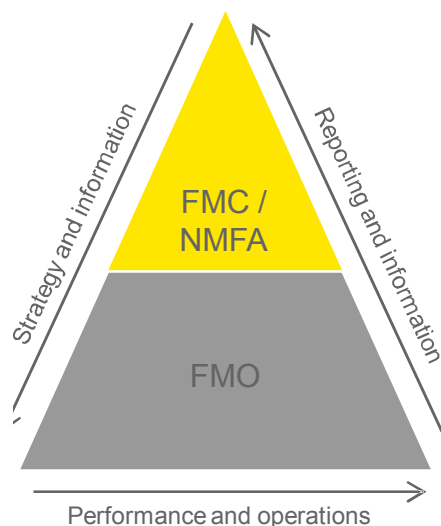
Risk reporting requirements communicated from NMFA to FMO are not clearly defined. It is communicated and requested on an ad-hoc basis. Reporting on risks from FMO to NMFA and FMC is considered appropriate and useful by the latter. The unsystematic manner in which risks are aggregated by FMO, poses a risk as to whether NMFA and/or FMC are provided a correct risk overview, especially given the ad hoc basis in which NMFA communicates its requirements. Risk reporting from program operators to FMO can be inaccurate and subjective, but we consider it appropriate and useful from a management perspective.

Information is communicated in an timely manner and provides a reasonable, if not completely reliable, basis for decision making. FMO director is not able to monitor performance and on the program area or sector level as there is no systematic production of such risk management information on those levels.

There is limited reporting from FMO to NMFA on measures and how identified risks are supposed to be addressed with appropriate measures. This is also consistent with our observations. FMO is relatively experienced and good at identifying and assessing risks, while there is a potential to improve how critical risks are addressed including reporting of mitigating actions.

Recommendations

12. The risk reporting from FMO to FMC and NMFA needs to be improved in order to give FMC and NMFA appropriate risk information. This is related to how identified risks are addressed and managed. FMC and NMFA need to be clear on what type of information they need and communicate this properly to FMO. The allotment letter and the management dialogues are important forums to address this challenge.



There are weaknesses related to preparing and reporting measures and mitigating actions for significant risks. It is necessary to identify, implement and follow-up risk mitigating actions and measures for critical risks. This must also be reported to important stakeholders such as FMC and NMFA to ensure proper monitoring and follow-up on prioritized risks. See also recommendation number 9.

The figure to the left shows the management pyramid where NMFA and FMC are responsible for setting the agenda and strategy, provide instructions and communicate needs. FMO on the other hand, is responsible for operations, execute the agenda and strategy, and communicate and report results.

2. Review of established framework for risk management in FM 2009-14

Risk monitoring

Program operators monitor projects within their program. Programs are continuously monitored by project managers in FMO. The monitoring guidelines are currently under development. Also, the NFPs and the National monitoring committees monitor the programs and reports to FMO's program managers. High-risk programs, beneficiary states and core processes that can potentially threaten objectives and strategy, are continuously monitored by their respective owners. FMO is able to implement measures such as freezing payment of funds, if serious risks are identified.

Recommendations

See recommendation number 9 and 12.

Reporting on irregularities

Irregularities are reported on a four-month basis by the program operators to FMO's program managers. This is done prior to any of the four-month payments schedule of the funds. The irregularities are logged on an aggregated level in FMO, and payments are blocked if any significant irregularities are reported, until the issues are resolved. The program operators also report on irregularities once uncovered by monitoring activities. An investigation is then opened if necessary. All irregularities are registered in a loss and incident register which forms the basis for implementation of measures related to identified areas of improvement. Reporting is done systematically and significant discrepancies are immediately escalated through the organization.

2. Review of established framework for risk management in FM 2009-14

Third party risk identification and assessment

Risk identifications and assessments are conducted on all levels in the grants scheme. This is the main risk management activity which is described throughout the documentation, and it is clearly mentioned who should be conducting it, and how often. However, there are no guidelines for how to perform these activities. Methodology is missing, leading to risk of different interpretations on the seriousness of identified risks, as well challenges in aggregating and reporting risks.

Each beneficiary state has a dedicated independent audit authority (i.e. auditor general, Ministry of Finance, internal audit, outsourced third party) which is responsible for conducting annual audits of all projects, as well as on a sample basis. The audits should assess the effectiveness of the management and control systems and submit their reports to FMC and NMFA.

Recommendations

See recommendation number 7 and 8.

Continuous improvement

There is a sound “lessoned learned” culture at all levels on the donor side of the EEA & Norway Grants. The initiatives taken based on the experiences of 2004-09, indicates this. The reorganization of FMO, the initiation of this project and the considerable work conducted in the established Regulations, as well as the introduction of result based management, further exemplifies this.

The continuous monitoring activities on all levels aim to provide information that can help inform decisions of key stakeholders to improve performance and results. Continuous improvement is deployed and integrated within the existing organization and its processes.

2. Review of established framework for risk management in FM 2009-14

2.3.5 Competence and capacity

Most of the people and organizations (FMO, FMC, NMFA, donor program partner) on the donor side management has sufficient competence. However they have limited capacity within their organization to conduct effective and efficient risk management. FMO has risk management included in many of its operational procedures, in addition to a risk management team. The capacity to conduct aggregations and thorough risk reporting, from FMO to FMC and NMFA, is limited. This is mainly due to the fact that sector and country officers currently do not have any detailed risk management activities in their job descriptions. It is likely that at least capacity, and probably competence, would be an issue if they had responsibility for risk management activities.

There is a risk that several of the people and organizations (NFP and program operators) on the beneficiary side of the grant management has limited capacity and competence within their organization to conduct effective and efficient risk management. This is also enforced by the lack of a clearly defined and common methodology and guidelines for risk management.

Members of FMO and some donor program partners, attended a course in results- and risk management in 2011. This course was held by the Norwegian Government Agency for Financial Management (DFØ), and two FMO staff members participated as resource persons and trainers. The course content was subsequently amended and held for all FMO staff.

2.3.6 Tools

DoRIS is a reporting system being developed which will cover all aspects of the grants management, from the program applications throughout the implementation, monitoring and evaluation. The intention is that the system will be used extensively by the program operators, NFP and FMO. It will be used by the beneficiary state to fill in data on the program proposals, as well as to report progress on the project and program indicators. FMO will track and monitor all data. The system will also detail the financial flow in each program, and FMO has the ability to stop the flow if results of their assessments and monitoring will necessitate it. The system has limited functionalities regarding risk management, as it does not have a pre-defined "risk language" when beneficiary states assess risks, nor has it any aggregation functionalities which enable FMO management, FMC or NMFA to see the aggregated risks in the programs.

3. Identification and analysis of risks in the donor side management of the EEA & Norway Grants

3.1 Overview of identified risks and measures

The table below shows critical success factors that need to be in place and handled carefully to succeed with the EEA & Norway Grants. Further, it shows potential risks and measures to mitigate these. In line with the review of the established risk management framework the findings are structured within the areas: Structure, People, Process and Systems.

Key findings are summarized below. The critical success factors, risks and measures are all identified through interviews with interested parties and are opinions of people working with the grants. The list can be viewed upon as a gross list of identified risks on the donor side management. At the current state the risks have not been assessed or prioritized. Recommended measures by Ernst & Young are marked yellow. Due to the project mandate we have not been able to assure FMO's compliance with the measures stated to be in place.

Legend:

- Current measures in place according to interviewees
- Recommended measures by Ernst & Young

Area	Topic	Critical success factors	Risks	Measures
Structure	Overall objectives	Realistic ambition level when defining objectives for the grants considering the relatively limited size of the funds compared to EU structural funds and the beneficiary states GDP.	Challenging to connect program and projects output to the grants objectives given the size of the funds compared to the overall size of the beneficiary states' economies.	Use of donor program partners and Norwegian project partners to improve the bilateral relations.
			Hard to measure the degree of success regarding the improvement of bilateral relations.	Develop methodology to measure the degree of success.
	Risk manager	Aggregation, follow-up and reporting of risks on country, sector and overall level.	No dedicated risk manager with a clear mandate to aggregate risks reduces the quality of risk information to FMC and NMFA which can lead to no or inappropriate measures.	Establish a dedicated risk management function in the FMO.
	Roles and responsibilities	Clear roles and responsibilities in the FMO program teams between the sector and country representative.	Unclear roles and responsibilities in the FMO program teams can lead to delays in the grant management process.	Define responsibilities in the program team.
	Legal framework	Consistent interpretation of the legal framework by all beneficiary states.	Different interpretation of legal framework leads to inconsistent outcomes of programs.	Legal framework is well articulated and communicated.

3. Identification and analysis of risks in the donor side management of the EEA & Norway Grants

Area	Topic	Critical success factors	Risks	Measures
Structure	Reporting	Integrated risk reporting between all countries, organizations and partners in the grants scheme.	Risks may be distorted in the reporting chain, meaning that the key messages in the risk assessments can be distorted in the exchanges between project operator, program operators, NFPs, FMO and NMFA.	NMFA and FMC need to establish a common “risk language” and implement this on all levels of the grant scheme associated with the grants. (See also section 2.3.3).
		Reporting of risks according to actual risks in country or program.	Under-reporting and downgrading of risks in projects/programs by beneficiary state stakeholders due to fear that high risk projects/programs will not get allocation of funds.	NMFA and FMC need to establish a common “risk language” and implement this on all levels of the grant scheme associated with the grants. (See also section 2.3.3).
		Clear and predictable governance to ensure efficient reporting and use of FMO resources.	Risk reporting from FMO to the NMFA can be suppressed by the latter due to political considerations which may cause reported risks to deviate from actual risks and appropriate measures not taken.	NMFA and FMC need to establish a common “risk language” and implement this on all levels of the grant scheme associated with the grants. (See also section 2.3.3).
		Predictable communication of priorities by FMC and NMFA to FMO.	Prioritization of programs based on political considerations with low probability of success.	Develop overview of political prioritized countries and programs developed by FMC and NMFA.

3. Identification and analysis of risks in the donor side management of the EEA & Norway Grants

Area	Topic	Critical success factors	Risks	Measures
People	Competence in FMO	High level of risk management competence in FMO.	Limited risk management competence in FMO pose a risk of inaccurate risk reporting.	Training and education of the FMO to improve risk management competence. Hire consultants and recruit personnel with risk management competence.
	Competence in FMC and NMFA	High level of risk management competence in FMC and NMFA.	Limited risk management competence in FMC and NMFA may weaken the overall management of the grants and reduce the rate of success.	Training and education of FMC and NMFA to improve risk management competence. Hire consultants and recruit personnel with risk management competence.
	Competence in the donor program partners	High level of risk management competence in donor program partners.	Limited risk management competence in the donor program partners pose a risk of delays and can reduce the grants' rate of success.	Training and education of the donor program partners to improve risk management competence. Hire consultants and recruit personnel with risk management competence. Establish a FMO helpdesk.
	Competence program operators	High level of risk management competence for program operators.	It may be challenging to identify suitable program operators in some program areas and beneficiary states.	Training and education of the program operators to improve risk management competence. Hire consultants and recruit personnel with risk management competence. Establish a FMO helpdesk.*

* The FMO helpdesk can be a service to the National Focal Points, Program Operators, Donor Program Partners, to give advice, counsel and contribute to appropriate risk management (I.e. by advising on templates, applications, risk assessments and different reports).

3. Identification and analysis of risks in the donor side management of the EEA & Norway Grants

Area	Topic	Critical success factors	Risks	Measures
People	Competence in the NFP	High level of risk management competence in NFP.	<p>NFPs are often Finance Ministries and unfamiliar with handling bilateral relations, which pose a risk of reaching the objective of bilateral relations.</p> <p>NFPs are often Finance Ministries with limited knowledge about the different program areas. This may slow the process and lead to funding of programs/projects with low probability of success.</p>	<p>Training and education of the NFPs to improve risk management competence.</p> <p>Hire consultants and recruit personnel with risk management competence.</p> <p>Establish a FMO helpdesk.</p>
	Capacity in the donor program partners	Donor program partners must have a high level of capacity in order to fulfill their role as defined in the Regulation.	Donor program partners do not have the necessary capacity and this impedes bilateral relations and reduces the quality of risk reporting from the beneficiary states and the donor program partners.	Allocation of funds to the donor program partners to ensure sufficient capacity.
	Job descriptions	<p>Job descriptions for all employees.</p> <p>Clear risk management responsibilities embedded in job descriptions.</p>	Job descriptions do not contain detailed risk management responsibilities and/or activities which lead to reduced reporting and follow up of risks.	Develop job descriptions, including risk management responsibilities, for all FMO employees.
	Cultural differences	<p>Utilize cultural differences to strengthen the grant management.</p> <p>Awareness of cultural differences and activities reducing these.</p>	Cultural differences may slow the grant management process and lead to delays.	Establish cooperation committees with donor program partners and beneficiary states, which can lead to an improved cooperation environment.

3. Identification and analysis of risks in the donor side management of the EEA & Norway Grants

Area	Topic	Critical success factors	Risks	Measures
Process	Proportionality	Strike the right balance between risk management and performance management.	Too much focus on risk management at the expense of performance management reduces the funds' desired outcomes.	Define risk appetite. Conduct risk assessments and prioritization of risks to find appropriate controls.
	Risk language	Develop and communicate common "risk language", including definitions, scales, categorizations and checklists for risk assessments.	Different "risk language" can lead to individual assessments of risks that reduce the quality of the aggregated risk assessments. High risk programs may receive low attention because risk assessments are inaccurate.	Establish a common "risk language" and implement this on all levels of the organization, contributing to risk management.
	Corruption	Monitor and follow-up of compliance with local legislation in procurement processes.	Corruption in public procurement processes reduce the success of the grant's overall objectives.	Transfer risks to beneficiary states by making them guarantee for the allocated funds. Assign donor program partners and donor project partners and delegate monitoring and reporting of risks.
Systems	IT systems	A well functioning IT system for documentation and reporting of risks is essential in order to aggregate and assess risks on a sector and country level.	Lack of reporting due to IT system challenges.	Development and implementation of DoRIS. Hire IT system experience for development, maintenance and help desk functionality.
	Data quality	Sufficient quality data provided on the project level in order to get adequate data output (reports etc.) on aggregated levels.	Insufficient data available from projects and defined indicators.	Training and education of the project- and program operators to improve risk management competence. Establish Norwegian project partnerships. Establish a FMO helpdesk.

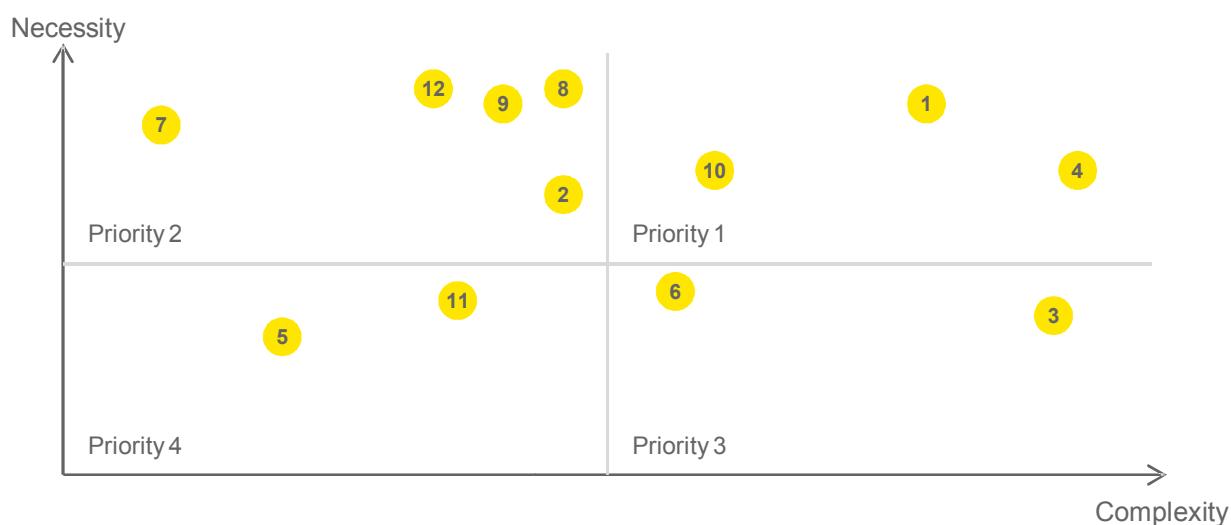
4. Recommendations

4.1 Prioritized recommendations

We have identified gaps in the current risk management framework in relation to leading practices. Recommendations are presented in the respective sections in the report, and are also shortly repeated in the table below.

We have reviewed and prioritized in terms of size, necessity and complexity. We have also indicated an overall proposal for the implementation plan of improvement proposals.

Recommendations in the upper right square requires most attention. These should have first priority and are also relatively complex to implement. First and third priority improvements often require establishment of projects. These measures require dedicated resources for an extended period of time. Second and fourth priority are more quick fixes and can be managed along with the daily operations.



Recommendations			
1	Risk management strategy	7	Job descriptions
2	Document hierarchy	8	Common “risk language” – scales and criteria
3	Reduce number of indicators	9	Measure plans
4	Define risk appetite	10	Risk aggregation
5	Risk management team mandate	11	Risk assessments in DoRIS
6	Risk manager function	12	Risk reporting

4. Recommendations

4.2 Next steps

In the risk assessment above we have identified areas of improvement and recommendations that we suggest to implement. In this part, the intention is to give the management of the grants input to conduct the suggested next steps. These steps might seem generic and this is intentional because the content should be provided by the organization itself (perhaps facilitated by an external third party). We therefore cover how, and why, the next steps can be conducted and suggest order of actions.

We suggest that the management start out by completing a risk management strategy (Recommendation #1). The risk management strategy must be initiated by FMC/NMFA and give clear guidance to FMO on how the risk management strategy is to be developed. We suggest that a project team consisting of members from both FMO, FMC and NMFA are responsible for developing the strategy.

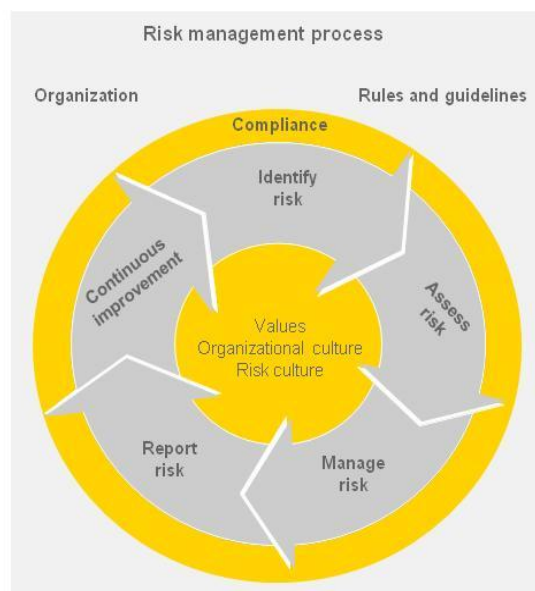
The purpose of the strategy is to give all relevant parties information and an understanding of what risk management of the grants is (and is not), why we perform it and how to approach it. The table on page 17 is an appropriate starting point when developing this strategy. This table only outlines suggested topics and it can be adapted to the grants' needs. Meanwhile, we strongly suggest that the strategy cover other suggested recommendations:

- ▶ Define a document hierarchy (Recommendation #2)
- ▶ Define a reduced number of indicators that are able to measure the degree of success towards the overall objectives (Recommendation #3)
- ▶ Define risk appetite for different categories, including an assessment of acceptable risk level or limits (Recommendation #4)
- ▶ Clear mandate for the risk management team (Recommendation #5)
- ▶ Establish a risk manager function (Recommendation #6)
- ▶ Define a common risk language, including criteria, and scales for probability and consequence (Recommendation #8)
- ▶ Describe the content of mitigating measure plans (Recommendation #9)
- ▶ Describe the appropriate level of risk aggregation and how to perform this (Recommendation #10)
- ▶ Describe which risk assessments that must be reported through DoRIS and how to conduct this (Recommendation #11)
- ▶ Describe general risk reporting principles, main reporting lines and frequencies (Recommendation #12).

4. Recommendations

To avoid that the risk strategy document becomes too comprehensive, we suggest that a separate document which describe the risk management process is developed and referred to in the strategy document.

The strategy for risk management is essential to have in place before a well functioning risk management process can be established. Recommended measures to implement a risk management framework is described both in part 2, 3 and 4 in this report. When a strategy is established the next step is to initiate the risk management process. The figure below shows an example of a risk management process.



The risk management process starts with identification of risks. This is followed by an assessment of the risk's implication and current efficiency of established internal controls. Then the principles for, and implementation of, detailed risk management and internal controls must be addressed. The last steps of the process is reporting and continuous improvement of the risk management process. In addition, implementation of measures to ensure compliance from the organization is important.

The table on the next page gives a more detailed description of the different steps in the risk management process.

4. Recommendations

Overview of risk management	Description
	Identify risk
	Assess risk
	Manage risk
	Report risk
	Continuous improvement
	Compliance

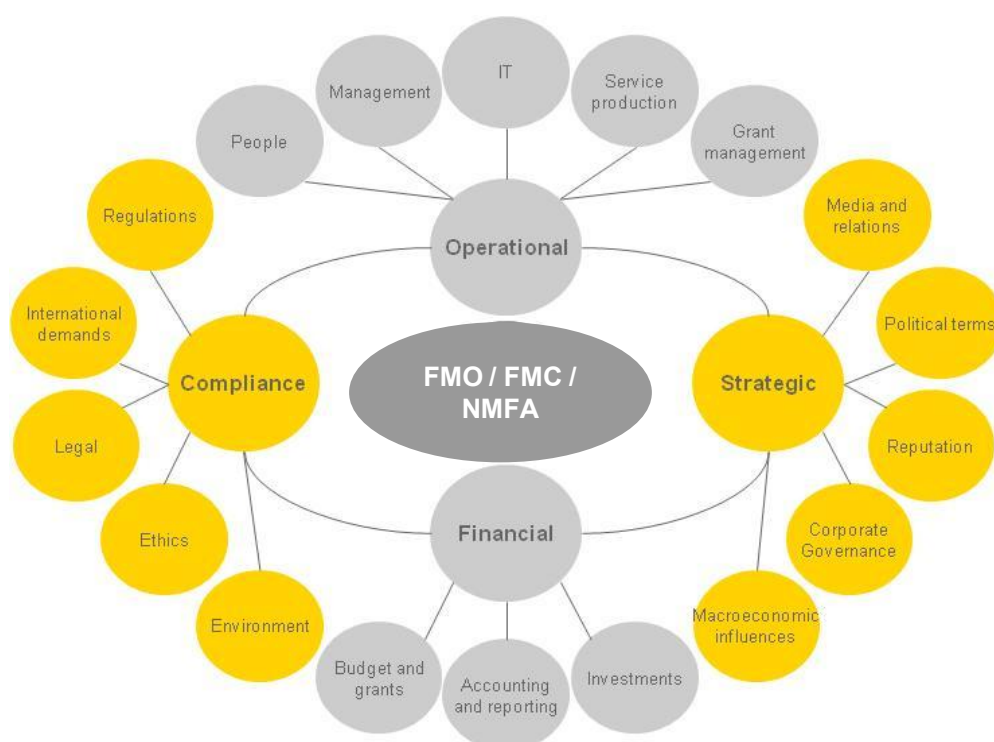
In the following pages we will elaborate on how the grant management can approach the different steps and show examples of relevant tools to conduct this.

4. Recommendations



Identify risk

The first step of the risk management process is to identify the grants' risk universe. The risk universe describes different risks related to categories. A suggested structure for the risk universe is described in the model below. Many of the relevant risks are described in part 3 of this report. The additional identification of significant risks can be conducted by a workshop with staff from FMO, FMC and NMFA.

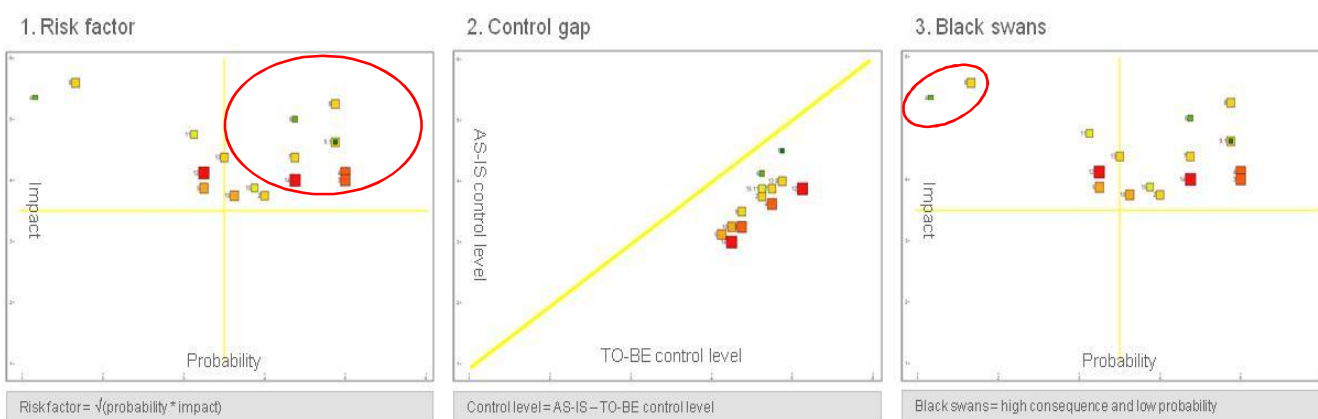


4. Recommendations



Assess risk

After all significant risks have been identified these should be assessed by considering probability and consequence. The assessment can be done by risk workshops or they can be made on an individual basis by for instance the program operators or program managers. Common risk language and competence is especially important when risk assessments are conducted by individuals. A risk assessment can also identify control gaps, which reflect the current control of a specific risk compared to the desired control. An example of how the output from a risk assessment can be presented is shown below:



The risk factor gives an indication of which risks the participants in the assessment considered to have a combination of high probability and high impact if they occur. Risks in the upper right quadrant is the area of focus and has a relatively high probability and impact.

The control gap gives an indication of the risks that the participants in the assessment considered to have too low level of control, and do not have the desired level of risk management. A large red plot in the risk map indicates a risks with a large control gap. All risks that are below the diagonal is assessed to have a too low control level and vice versa.

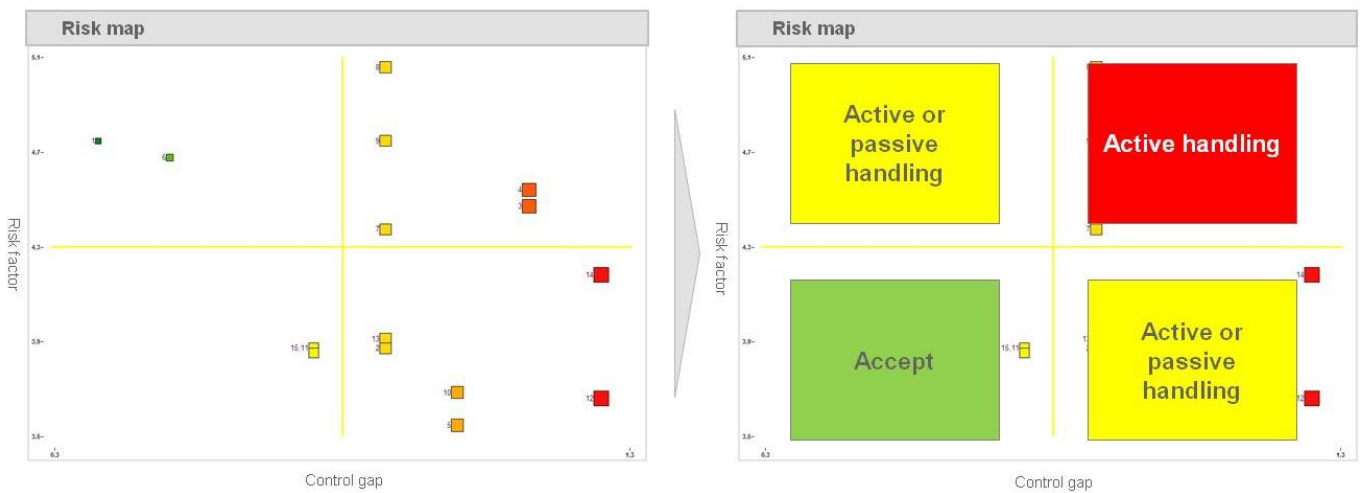
Black swans occur rarely, but if it happens the risks will have critical impact for the organization. The organization should assess what types of potential black swans it can be exposed to.

4. Recommendations



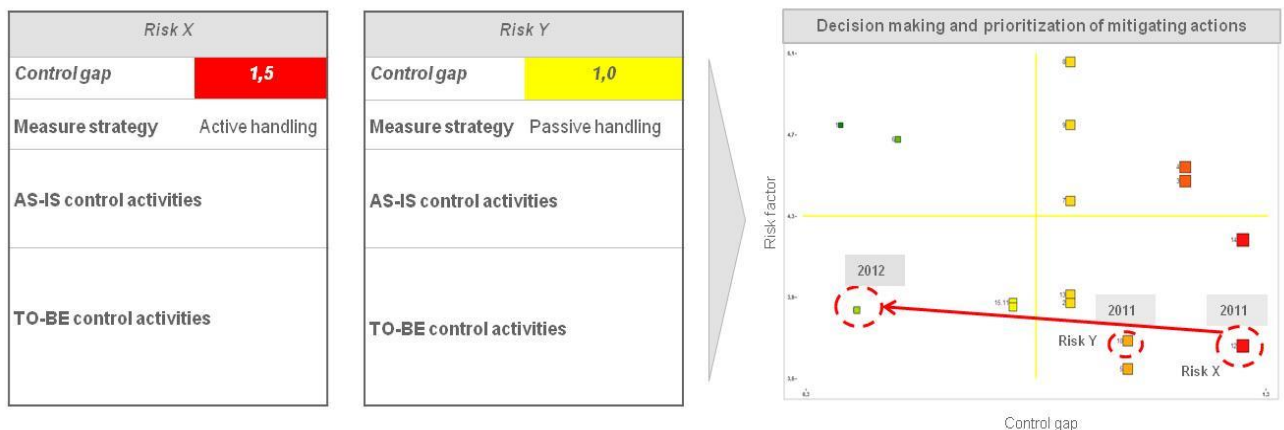
Manage risk

Risk assessments are important when it comes to managing risk because they give a clear indication of where the significant risks are and which should be prioritized. The risk appetite for different categories, defined in the risk management strategy, compared to the control gap will give crucial input to the prioritization of the risks. Examples of risk maps are shown below with generic comments on how to handle different areas of the risk map. It is worth mentioning that the decision of active versus passive risk handling is a matter of discretion.



1. **Active handling:** Normally mapped first. Requires follow-up with concrete measures to reduce the control gaps, probability, and /or impact.
2. **Passive handling:** Risks in these quadrants are normally not the first priority. Passive management is often practiced through monitoring and reporting of risks.
3. **Accept:** Normally accepts that these risks occur. When the risk factor and control gap is relatively low, there is less need for concrete measures.

A mitigating measure plan can be initiated when the significant risks are prioritized. The prioritized risks must be evaluated in terms of the current or “as-is” control activities, compared to the future or “to-be” control activities. A plan for reaching the future state can then be mapped by implementing appropriate control activities. An example of this is shown in the diagram below.



4. Recommendations



Report risk

Significant risks must be aggregated and reported to relevant levels of the organization. Based on preferences from FMC and NMFA this can be done by aggregating risks on programs, program areas, beneficiary states or a combination of the these. The most critical risks can for example be presented to the FMC and NMFA in a dashboard consisting of two different risk maps and a table of the rolling top 10 most important risks. This is shown in the diagram below:



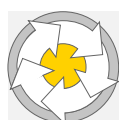
In addition to the risk management dashboard the reporting of risks should include a description of the mitigating measure plan for the most significant risks. Clear reporting lines and frequently reporting is a crucial success factor and this must be defined in the risk management strategy.

4. Recommendations



Continuous improvement

The last step of the risk management process is continuous improvement which means that the risk management process should be evaluated on a frequent basis to develop the process even further and enable learning.



Compliance

Compliance is important for all steps in the risks management process. To ensure compliance the FMC and NMFA can initiate self-assessments and independent audits.

We have now given an overview of the recommended next steps, except for one, based on the prioritized recommendations. The last recommendation is regarding job descriptions, which has low complexity and relatively high necessity. FMO is currently in progress of reviewing all job descriptions.

Appendix A – Maturity charts

Strategy and policy

	1	2	3	4	5
Focus Area	Basic	Evolving	Established	Advanced	Leading
Risk management strategy and policy Current score: 3	The strategy and policy are not established, formalized, communicated or deployed.	•	•	•	•
Objectives and KPIs Current score: 4	Objectives and KPIs are established on the EEA & Norway Grants level only.	•	•	•	•
Risk appetite and risk limits Current score: 2	Risk appetite and risk limits are not defined on any level.	•	•	•	•
				The strategy and policy are well established, formalized, well communicated and consistently deployed. Strategy and policy are continuously developed to recognize changes in the organization and external environment in order to drive and achieve leading performance.	
				Based on the grants vision and strategy, specific targets are defined and translated into a set of operational and financial objectives and KPIs, which build upon relevant and well-defined drivers. These objectives and KPIs are established on the aggregate EEA & Norway Grants level, as well as on program, country and project levels. Plans, budgets and forecasts are based on these KPIs. The KPIs are applied consistently throughout all projects.	
				Risk appetite and risk limits are defined on the EEA & Norway Grants level as well as on the program, project and beneficiary state level. The risk appetite and the risk limits are clearly linked to the established objectives and KPIs and they are reflected in the controls and authorities defined.	

Appendix A – Maturity charts

Roles and responsibilities

Focus Area	Basic	Evolving	Established	Advanced	Leading
<p>Overall organization of roles and responsibilities</p> <p>Current score: 3</p>	<p>Roles, activities and responsibilities regarding risk management are loosely defined and not documented. Roles, functions, responsibilities and tasks lack clarity and transparency.</p>	•	•	•	•
<p>FMO organization of roles and responsibilities</p> <p>Current score: 3</p>	<p>Roles, activities and responsibilities regarding risk management are loosely defined and not documented. Roles, functions, responsibilities and tasks lack clarity and transparency.</p>	•	•	•	•
<p>Job descriptions and authorization levels</p> <p>Current score: 4</p>	<p>Unclear roles and responsibilities are highly disruptive to the organization's performance. Authorization levels are not in place or are not communicated. The organization lacks segregation of duties.</p>	•	•	•	•
				<p>Roles, activities and responsibilities regarding risk management are fully and mutually aligned between the Ministry of Foreign Affairs, FMC, FMO, beneficiary states, and program and project levels.</p>	
				<p>Roles, activities and responsibilities regarding risk management are fully and mutually aligned between the different positions within FMO. There is a dedicated risk management function in FMO which define, aggregate and report risk management activities in the donor management process.</p>	
				<p>Formalized job descriptions for all roles and employees are established. The job descriptions are regularly reviewed and updated. Authorization is limited to a single process. All employees are able to access relevant policies, procedures, working instructions and manuals on-line.</p>	

Appendix A – Maturity charts

Routines and methodology

Focus Area	Basic	Evolving	Established	Advanced	Leading
<p>Description of routines and procedures for risk management</p> <p>Current score: 3</p>	<p>Descriptions of routines and procedures for risk management are not established.</p>	•	•	•	•
<p>Risk assessments of applications and distribution of grants</p> <p>Current score: 4</p>	<p>Risk assessments of the applications and distribution of grants are not conducted.</p>	•	•	•	•
<p>Categorization and aggregation of risks</p> <p>Current score: 3</p>	<p>There are no categorization and aggregation of risks at any level.</p>	•	•	•	•
<p>Standardization of risk management templates and tools</p> <p>Current score: 3</p>	<p>Templates and tools have individual ownership and do not include relevant risk management aspects.</p>	•	•	•	•

Appendix A – Maturity charts

Reporting and monitoring

Focus Area	Basic	Evolving	Established	Advanced	Leading
<p>Risk reporting system</p> <p>Current score: 3</p>	Risk reporting is driven by external requirements that are not sufficiently defined or produced for management and/or other stakeholders. Pertinent information is not communicated.	•	•	•	•
<p>Risk management information</p> <p>Current score: 3</p>	There is no relevant information on risks reported to FMC or FMO.	•	•	•	•
<p>Irregularities reporting</p> <p>Current score: 5</p>	No established system for registering and reporting of identified irregularities from defined objectives and KPIs. Loss and incident register does not exist.	•	•	•	•
<p>Risk monitoring</p> <p>Current score: 3</p>	Monitoring of risk is performed randomly and on an ad-hoc basis.	•	•	•	•
<p>Third party risk identification and assessment</p> <p>Current score: 5</p>	Risk identification and assessments do not occur on a structured and consistent basis within the organization.	•	•	•	•

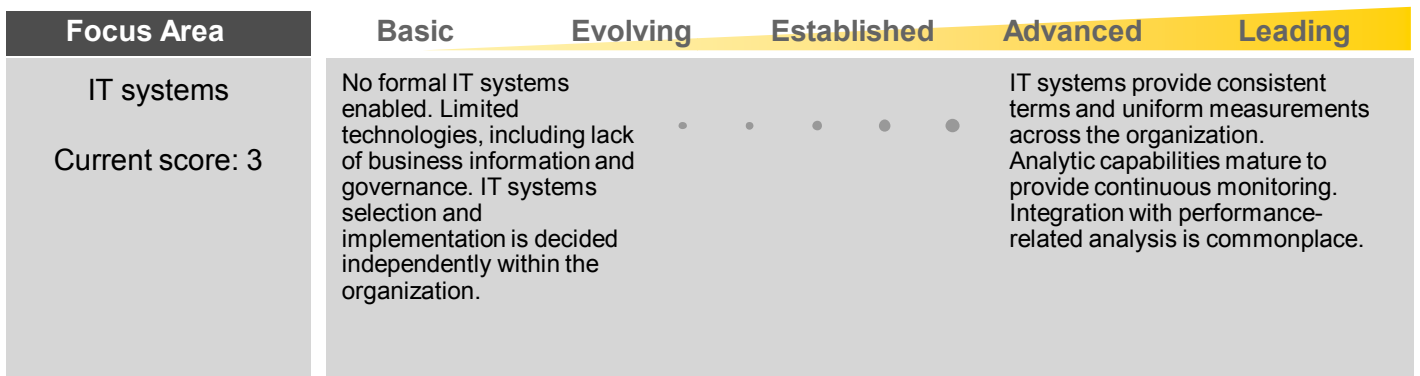
Appendix A – Maturity charts

Competence and capacity

Focus Area	Basic	Evolving	Established	Advanced	Leading
<p>Risk Management on the agenda</p> <p>Current score: 4</p>	<p>Risk Management is not on the agenda with management- and team meetings.</p>	•	•	•	•
<p>Competence and capacity on the donor side</p> <p>Current score: 3</p>	<p>None of the interested parties (FMO, FMC, NFMA, DPP) on the donor side of the grant management have sufficient competence and capacity within their organization to conduct effective and efficient risk management.</p>	•	•	•	•
<p>Competence and capacity on the beneficiary side</p> <p>Current score: 3</p>	<p>None of the interested parties (NFP, PO's) on the beneficiary side of the grant management have sufficient competence and capacity within their organization to conduct effective and efficient risk management.</p>	•	•	•	•
				<p>Risk Management is permanently on the agenda with management- and team meetings. Periodically an overall business risk-profile is generated and reported to FMO and FMC.</p>	<p>All interested parties (FMO, FMC, NFMA, DPP) on the donor side of the grant management have sufficient competence and capacity within their organization to conduct effective and efficient risk management.</p>
				<p>All interested parties (NFP, program operators) on the beneficiary side of the grant management have sufficient competence and capacity within their organization to conduct effective and efficient risk management.</p>	

Appendix A – Maturity charts

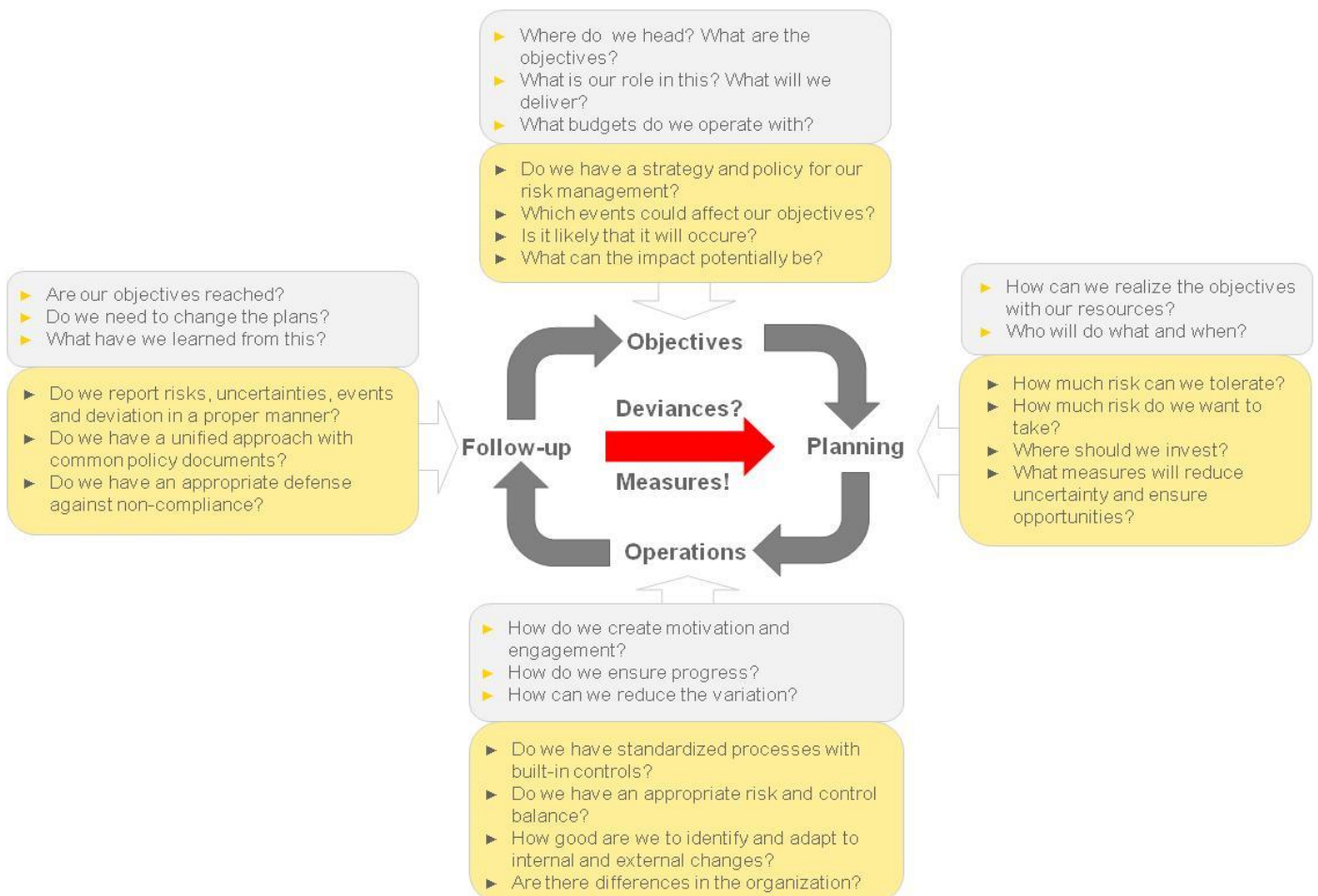
Tools



Appendix B – The link between performance management and risk management

How risk management and performance management are related

The figure below shows the four key components in a performance management model, also with reference to risk management. We show some key questions that need to be addressed in order to determine the integration of risk management (yellow boxes) and performance management (grey boxes). This figure also shows the differences and similarities between risk management and performance management.



Appendix C – Abbreviations and definitions

FM	Financial Mechanism
FMC	Financial Mechanism Committee
FMO	Financial Mechanism Office
NFM	Norwegian Financial Mechanism
NFP	National Focal Point
NMFA	Norwegian Ministry of Foreign Affairs
MEUR	Million Euro
COSO	The Committee of Sponsoring Organizations of the Treadway Commission

Risk: Risk is defined as any event or circumstance that creates uncertainty around the expected achievement of the organization's objectives. The event may trigger a positive or negative result that the organization may experience in pursuit of its mission, vision and strategic direction.

Inherent Risk: Inherent risks are those risks that are likely to occur and would impact upon the organization's objectives without consideration of any controls in place to mitigate the risk.

Risk management: The identification, assessment, and prioritization of risks defined as the effect of uncertainty on objectives, whether positive or negative, followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.

Risk appetite: The broad-based aggregate ability to deliver amount of risk an organization is willing to accept in pursuit of its mission, vision and objectives - directly related to an organization's risk capacity as well as its culture, desired level of risk, risk management capability and business strategy.

Risk tolerance: The specific *maximum* applicable to each category of risk regarding the magnitude of risks that *the organization is willing to take* to achieve its strategy and objectives - set such that the aggregation of risk tolerances ensures the organization operates within the risk appetite.

Appendix C – Abbreviations and definitions

Risk targets/limits: The optimal level of risk that the organization desires to take to achieve specific business objectives and operate within its appetite/tolerance for risk. Thresholds to ensure that variation from expected outcome will be consistent with the risk target, but will not exceed the risk appetite – defines process level controls and management authorities.

Risk drivers: Risk drivers are the causal drivers of risk that affect the severity of impact of the event or circumstance.

Risk factor/exposure: Captures the effect of the impact assessment and the probability or frequency of occurrence for a particular risk. It is calculated by square root of multiplying the impact rating with the likelihood rating.

Control gap: Captures the effect of deviance between established controls (AS-IS) and optimized controls (TO-BE). It is calculated by subtraction of the TO-BE and AS-IS ratings.

Critical success factors (CSF): is the term for an element that is necessary for an organization or project to achieve its grand objectives. It is a critical factor or activity required for ensuring the success of a company or an organization. CSFs include issues vital to an organization's current operating activities and to its future success. Success criteria are defined with the objectives and may be quantified by key performance indicators (KPI).

COSO ERM: Enterprise risk management framework, providing key principles and concepts, a common language, and clear direction and guidance.

Key performance indicators (KPI): A set of quantifiable measures that an organization uses to gauge or compare performance in terms of meeting their strategic and operational goals. An organization must establish its strategic and operational goals and then choose the KPIs which best reflect those goals.

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 150 000 people - 1 600 in Norway - are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

www.ey.com

© 2011 EYGM Limited
All rights reserved

