IIA Norge

An Introduction to Operational Risk Management

1st Edition 2022

What is governance?

An interaction of responsibilities involving owners, the Board of Directors and management in a long term and sustainable perspective. The aim is to ensure that the enterprise creates value, achieves its objectives, and complies with laws and regulations. It encompasses the structures, processes and tools which are used to manage activities, resources, and risk in an enterprise.

Internal audit

The instrument of the Board of Directors for enhancing and protecting organisational value by providing risk-based and objective assurance, advice, and insight.

Compliance

Compliance refers to complying with applicable laws and regulations both nationally and internationally as well as the enterprise's internal policies. A focus on compliance risk also contributes to strengthening adherence and increased awareness of compliance in the enterprise. It is a legally required function in the banking and finance sector.

Risk management

An enterprise-wide and proactive risk management is key to good governance. This process helps to ensure the best possible decision basis at the strategic level in the enterprise. It covers both potential negative and positive outcomes.

Content

1 Definition and introduction

1.1 What is operational risk?

Most enterprises will pursue and strive for an effective business model which maximises the possibility of achieving the organisation's objectives. The enterprise may have a range of objectives which are not automatically limited to financial and business goals, such as in the areas of social responsibility and sustainability. Operational risk concerns being conscious of to what extent *operational choices and related operational risks* may arise on the road to achieving all of these goals.

There are many definitions of operational risk. In these guidelines the four dimensions of protection of physical assets, people, organisation and technology form the basis of the definition of operational risk, because it has been shown that the root cause of operational risk events are often connected to these dimensions.

These conditions can either result in an upside or downside effect and contribute to increasing or reducing the probability of an organisation achieving its overall objectives.

The following definition therefore forms the basis for the concept of operational risk and related concepts in these guidelines:

Operational risk applies to physical assets, people, processes and the use of technology in performing the daily activities and service provision of the enterprise and can result in both positive and negative outcomes. This includes the treatment of uncertainties, possibilities and risks in the day to day operations as well as the consequences of undesirable events.

The outcomes can also arise because of external events (technology, trends, legal requirements, political expectations) and is also connected to decisions taken under existing conditions and based on a limited information basis. The outcomes experienced can be disandvantages (downside), gains and/or increased utility (upside).

Uncertainties relate to unspecified values or insufficient information.

Risks are specifically defined values within given expectations, whilst possibilities are an unexploited upside potential until they are actively realised.

In a complex world with constant change the importance of Operational Risk has increased and is on the agenda of the Board of Directors and executive management. Typical factors encountered in Operational Risk Management are:

a) The use of technology both in the form of traditional data processing and in the new areas of AI (Artificial Intelligence), IoT (the Internet of Things), the metaverse, blockchain etc. as well as integrated digital services.
b) Changes in legislation (e.g. the Transparency Act, GDPR and outsourcing to non-EU countries – Schrems II).
c) Ever more complex data structures and automated processes.
d) The competitive environment driving mergers and acquisitions.
e) External threats such as war, pandemic, cyber crime, and mental health.
f) Internal re-organisations are the new norm for addressing requirements and expectations.
g) Outsourcing, third party suppliers and supply chains as well as the associated requirements related to human rights.

In addition to internal requirements:

h) To increase operational quality.
i) To improve the management and control of interfaces and internal and external data transfers.
j) To reduce the probability and consequence of undesirable outcomes.
k) To adress regulatory requirements and expectations in an effective manner.
l) Physical security of buildings including protection against burglary, theft and fire.

1.2 Why is it important to practise operational risk management?

The objective of risk management is to support decision making and find the best options and possible solutions for the enterprise given its context, organisational ability and financial capacity. Operational Risk Management is therefore an important part of governance.

Risk adresses uncertainty associated with future developments. The outcomes can be better or worse than we had planned or assumed. This is where operational risk has a potential upside as management can be improved through a more applicable and effective management and control. Enterprises may achieve this through increased awareness of the factors contributing to goal achievement, knowledge of what can go wrong and how to control these areas, as well as identifying which areas can be improved by increased automation or other organisational changes.

Operational Risk Management helps us to define and understand risks (threats and opportunities), so that we are able to make better decisions at all levels within the enterprise in order to achieve the objectives set by the enterprise itself.

1.3 The function for operational risk management – ensuring a common framework

The guidelines for the risk management function published by IIA Norway address and define the risk management function that will have the role of providing a «a systematic and objective approach to identifying, analysing and evaluating risk as well as designing and implementing activities which will allow risks to be managed within defined risk targets». A separate function is often the result of legal requirement. For other enterprises (both private and public) it is important that management is in charge of Operational Risk Management, but often with the support of a risk

function. It is important that both management and process owners have ownership of the management of risk within their responsible areas/processes.

A common framework for Operational Risk Management should include the following:

- A high level policy including the setting of goals for operational risk management (e.g. to reduce costs, increase quality over time, improve decisions) and the definition of roles and mandate as well as securing the function's authority (independence).
- A consistent and defined process which will underly how the involved parties shall coordinate internally and define their planned activities, and which will form the detailed requirements in the following areas:
  - Knowledge
  - Capacity
  - System tools.
- Required instructions, either included in a process description or through concise and concrete governing documents which are comprehensive, agreed upon and approved. These should address:
  - The effective division of responsibilities between the centralised function and line management for performing the risk management activities.
  - Assistance to and education of line management which will reinforce a sound culture and improvement of attitudes.
  - Regular reporting to executive management of the status in respect of planned activities and changes to this plan.

The concrete definition of the Operational Risk Management will depend on the size and requirements of the organisation, and the management model. For example it will often happen that a large and complex organisation has a department headed by a Chief Risk Officer (CRO), whilst a smaller organisation may allocate this responsibility to another function such as, for example, a Controller or Chief Financial Officer (CFO). The main point is that someone in the enterprise should be identified and given a dedicated responsibility for operational risk and with a defined mandate. Similarly the responsibility for operational risk should be clearly identified and be recognised by executive management and ultimately the Board, thus ensuring that operational risk is an integrated part of the enterprise's management processes and aligned with other governance activities.

Larger organisations often find it advantageous to have a separate organisational unit for Operational Risk Management where the manager and staff report to the CRO or Head of Quality and Risk, whereas in smaller organisations operational risk management is a part of another function with overall responsibility for Enterprise Risk Management, financial control, operational and/or quality management. In mature organisations it is common to find a defined operational risk appetite with related tolerance limits for the various parts of the operational risk universe.

The likelihood of achieving a good and cost efficient operational risk management will increase if the responsibility for a common Framework for Operational Risk Management has been allocated and a function/role established with responsibility to maintain this with possibly the support of a technical systems solution. This will apply regardless of the size and organisation.

Figure 1: The relationship betwen governance and Operational Risk Management

In this document we find that there is a connection between Operational Risk Management and governance.

Risk management and internal control should be established within all appropriate risk areas, including within the area of operational risk. The key point is that the operational risk profile must be seen in context with the organisation's other choices and priorities as an enterprise-wide portfolio of risks.

2 Proposed model for working with Operational Risk Management

The core of all risk management is what is commonly called an action plan. Some people also call it a risk management plan.

The action plan is an overview of those activities which will contribute to the treatment of risk and thus increase the likelihood of achieving objectives and positive outcomes.

Operational Risk Management encompasses in practice the following processes:

1) Establish a risk-based action plan which is aligned with the enterprise's objectives,
2) Implement the action plan,
3) Monitor and report, as well as
4) Evaluate and adjust the action plan.

In total this can be illustrated in the following four stage model:

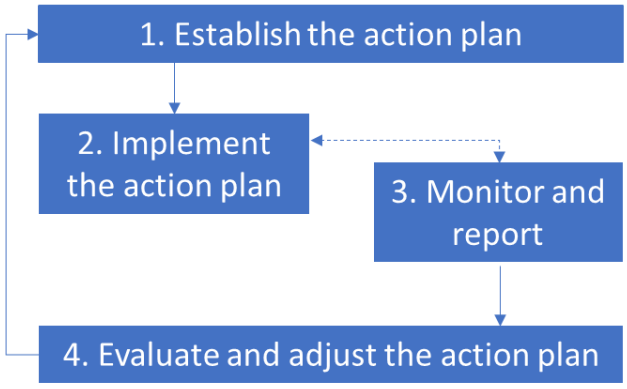
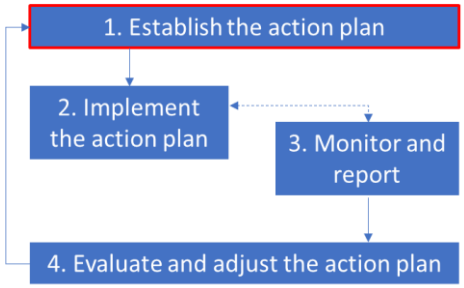


Figure 2: The four-stage model for working with Operational Risk Management

In the following, each stage will be described separately.

2.1 Establish the action plan

Most enterprises will establish project plans to manage their projects, a business plan to manage strategic activities, a marketing plan to manage customer centric activities or a financial plan to manage investments, capital, and liquidity, but how many enterprises establish separate action plans to manage their operational risk?



Establishing an action plan is a matter of defining those activities which the enterprise believes to be the most important to prioritise in the management of operational risk.

To accomplish this, it is necessary to be able to identify, describe and evaluate the most important operational risks – i.e. the potential events or circumstances linked to people, processes or systems which could result in positive or negative outcomes on the road to achieving set objectives. In connection with this it is important that effort is made to quantify risk in monetary terms, this can also include an assessment of quality costs, so that you can both prioritise where to put in effort and evaluate the cost/benefit of proposed activities. This will also include deciding which parts of an

enterprise's operations should be outsourced or insured because the enterprise has neither the capacity nor the ability to bear these risks.

Furthermore, the enterprise must be capable of implementing and documenting the risk management process. Documentation is a visual proof of a structured approach, even though documentation is not the aim of the exercise it is actions implemented in reality which count. The exception can be in the compliance area where there may be legal requirements regarding documentation which require the underlying evaluations and assumptions to be demonstrated in a systematic and structured way.

An action plan will not be better than the quality of the risk assessment performed, in which assets, vulnerabilities and threat scenarios are grouped into concrete risk descriptions.

The most important success criterion in this stage is knowledge (cf. chapter 1 concerning a common framework for operational risk management) in respect of the enterprise itself and its current threat landscape. Knowledge of your own enterprise and value generated through core and support processes, as well as commitment to compliance is a necessary precondition for the enterprise to be able to:

1. Articulate clearly what effect the identified potential events or conditions may have on the enterprise.
2. Prioritise these potential events or conditions in relation to one another.
3. Evaluate how the enterprise may realistically treat the prioritised potential events or conditions should they become reality – concretely what assumptions regarding capacity must be realistically in place for the risk to be treated.
4. Evaluate whether processes and controls can be improved, for example by simplification or automation.

Without sound understanding of the enterprise itself including the current threat landscape and possibility area there is a danger that the action plan will consist of irrelevant activities which are not capable of being operationalised in practice.

In order to arrive at good and relevant risk descriptions the enterprise must take as its starting point how it is proposed in practice to arrive at the business objectives – more precisely how it is envisaged to organise physical assets, people, processes, and technology to achieve the set objectives. After clarifying this it is possible to take the typical attributes listed under a) to l) in chapter 1 and evaluate to what extent each individual factor may affect the process of achieving the objectives. Where one or more of these attributes can have a strong impact over the operation(s) on the road to goal achievement then the potential activities should be identified and defined.

Activities should then be evaluated and agreed on. It is tempting to assume that one should choose the road to the goal which is at first glance the safest. This is where the upside/possibility aspect comes in and the importance of performing a good cost/benefit assessment of proposed activities. In this respect it becomes important to endeavour to quantify the proposed activities and evaluate them against the risk assessment expressed in monetary terms. The situation may arise where another way of organising physical assets, people, processes, and technology which is maybe "less

safe" but at the same time means potentially lower costs, shorter time to market, better quality etc. This means in reality that the enterprise must estimate the cost of designing, implementing, and monitoring each single action. This estimate must be evaluated against the possible benefit, or effect, that it is expected the activity will have on the ability to achieves the objective. One way of evaluating the effect of proposed actions is to establish and monitor relevant KPIs[1] including significant deviations/events.

The "deliverable" from this first stage will be well-reflected, prioritised and goal-oriented actions which the organisation believes will have a positive outcome for an acceptable level of investment.

A typical pitfall when performing a risk assessment is that the risk descriptions are too quickly arrived at and imprecise. Good risk descriptions are a pre-requisite for the assessment and action plan being precise enough so that the organisation can evaluate realistic or plausible scenarios which the enterprise must have under control.

There will always be external risks which are completely unknown or emerging, or areas where there is insufficient data and/or basis for assessment, and these must be dealt with separately to distinguish these from more known risks in internal processes, systems, and the organisation.

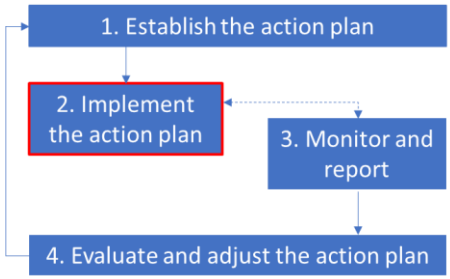
Some of the risk areas will also be covered by various insurance programmes as downtime and various types of shutdown can lead to major financial consequences for the enterprise as a whole.

2.2 Implement the action plan

In the final phase of establishing the action plan it is important to make estimates of the underlying activities/resources needed to implement and monitor each proposed action. The implementation of the described chosen actions may be described as active risk management.

The most important success criteria at this stage are that:

- The actions have defined, named owners who can ensure good progression in the actions they have responsibility for.
- The owner of an action has the competence, authority and capacity required to ensure the requisite progress.



The possibility of ensuring the function has adequate knowledge, authority and capacity should be addressed in the enterprise's overall policy, which should inter alia define roles and mandate (cf. chapter 1 concerning a common framework for Operational Risk Management).

[1] KPI = Key Performance Indicator

A clear and concise mandate reduces the chance of areas of doubt, unclear responsibilities, and unnecessary conflicts in performing the work of implementing and monitoring activities in the action plan.

Given the starting point of adequate knowledge, authority, and capacity the owner of one or more of the activities in the action plan should be in a position of leading and monitoring the actions including gathering and managing the resources required to complete them. It may well be the case that several activities can be consolidated into one concrete project, with its own organisation, performance measurements, and reporting in line with the enterprise's own project model. In all cases the person responsible for a defined action should ensure that the following items are delivered in order to ensure an effective implementation of their own activities in the action plan:

1. Define and assure the quality of assumptions underlying the successful delivery of the action, including ensuring that there is an adequate human resources, competency and financial budget.
2. Define the attributes of the action point upon completion.
3. Clarify and agree on the plan/timeline for the activity, including organisation and any dependencies that may be relevant.
4. Define a time limit for when the action shall be completed.
5. Detail who will confirm or approve the action which has been completed.

The "deliverable" from this second stage will be that all the agreed actions are either implemented as planned, or alternatively delayed or terminated because of a decision taken during the design/development phase, so that the action is no longer considered to be relevant or worth the effort of completion.

A typical pitfall within risk management is lack of recognition or prioritisation of the importance of defining ownership clearly and allocating responsibility internally. Ownership of both risks and the associated activities in the action plan shall ensure an evaluation of realism in the plans established as well as allow for the monitoring of delivery. In addition to this it will avoid the temptation of making a long action list which is lacking in priority, monitoring action or validation of the outcome and expected benefit.

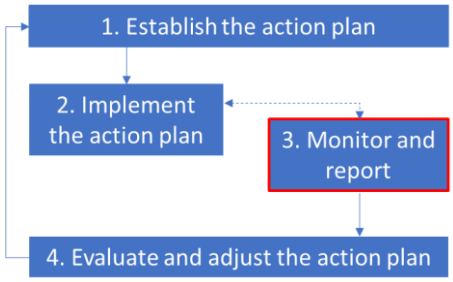
Another typical pitfall is the underestimation of the importance of discussing, approving, and documenting what are the necessary pre-requisites to be able to deliver the defined action. In such circumstances the planned action can be incorporated into the ordinary line management responsibility without allocating the resources to complete the task. The knock-on effect of such a situation is that the activity is in a fight for resources with the other line management activities that the person has responsibility for. This will result in turn in a lack of priority that it was assumed the action should have based on the operational risk assessment.

The importance of discussing, approving, and documenting the requirements necessary to be able to deliver approved actions should not be underestimated.

2.3 Monitor and report

This stage concerns monitoring in two dimensions/separate levels:
In the one dimension it concerns the monitoring of status of the agreed actions and ensure good coordination and communication of the extent to which the involved risk owners and persons responsible for the actions are on course in respect of the activities agreed in the action plan.

In some ways this stage can be seen as supporting implementation of the action plan, cf. especially point 3 in the 5 point list for the person responsible for an action in chapter 2.2 (namely to clarify and agree on the plan/timeline for the activity, including organisation and any dependencies that may be relevant).



In the second dimension, this stage concerns monitoring and reporting on factors that make it possible for the enterprise to evaluate and if necessary, adjust the basis of the action plan – i.e. the operational risk profile. This stage can therefore also be seen as the basis for the enterprise's ability to adapt and tailor operational risk management to make it as efficient and effective as possible.

2.3.1 Monitoring and reporting on activities

The most important success criteria for this stage are that:

- Routines and commitments are defined as to how monitoring and reporting shall be carried out, including both to whom and how often and with what content as well as the procedure for escalation.
- There is a simple shared arena/platform for communication and coordination across those involved in operational risk management.

It is often best to decide on routines and allocate commitments in connection with or based on the work with a process description and concrete and goal-oriented instructions.

A satisfactory arena/platform for collaboration may be achieved by agreeing on fixed meetings for review and reporting ideally with the support of a system which is familiar to and can be used by all the involved persons. Cf. chapter 1 concerning the requirement for a common platform for operational risk management.

The fact that monitoring and reporting is in this document described as a separate stage, indicates that actions may for various reasons be delayed or become more difficult to implement than expected or planned. In these situations, it will become apparent how successful one has been with the planning and allocation of knowledge, capacity, mandate, and authority of those performing the tasks.

A typical pitfall is that effort has not been made to establish a good compliance practice of approved governing documents. In such a case the result is the existence of a theoretical framework which describes "how we do it here" – but where actual practice is something else.

This is often revealed when the person responsible for an action does not have the ability to implement something which according to the framework they should have and/or that monitoring and reporting does not reach out to the relevant stakeholders. Because of this the person responsible for the action is left treading water and there is no easy access to the decisionmakers who should be able to intervene to amend the access to resources and ensure progress. Consequently that person, despite the preceding stages, does not have sufficient ability to ensure completion. Ending up in this situation may be avoided by establishing an escalation procedure and effectively dealing with the challenges hindering completion of the action.

The design of a good culture for deviation reporting in the implementation process is important for the successful management of operational risk and where necessary practice should be amended.

2.3.2 Monitoring and reporting on the action plan

This stage concerns collecting information about and reporting on matters which make it possible to evaluate and adjust the action plan in line with the development of the enterprise's processes, context, and threat landscape.

Quality in the action plan and thus in operational risk management will not be better than the ability to identify and use information about the current operations and business context.

An important success criterion for this stage is knowledge of your own enterprise and the current threat landscape in the same way as it was when the action plan was being established. When establishing the action plan, it is important to have knowledge of the current situation. In monitoring and reporting it is rather a matter of obtaining an overview and knowledge of changes in pre-existing conditions or the introduction of new conditions which can affect operational risk. In other words, this criterion of success is related to the ability to measure and identify conditions involving the four dimensions of physical assets, people, organisation, and technology.

Below we have listed some of the most important subjects which should be considered included in performance measurements:

- Monitoring of the implementation of action plans and (improvement) projects (actions to reduce risk, cf. chapter 2.3.1 above)
- Analysis of KPIs related to operations, quality and deviation reports identifying possible root causes including the follow up actions of events, production time, back log, error percentages, irregularities, leakage and other forms of fraud, customer complaints, sick days, employee satisfaction etc.
- Changes in contextual conditions e.g. access to raw materials, changes in technology, external events such as natural disaster, incidents of cybercrime etc. The basis for this reporting should be the insight that the operational risk management function gains through monitoring relevant media, professional forums, unwanted events both internally and externally etc.

These performance indicators can be further detailed/categorised into the relevant areas of physical

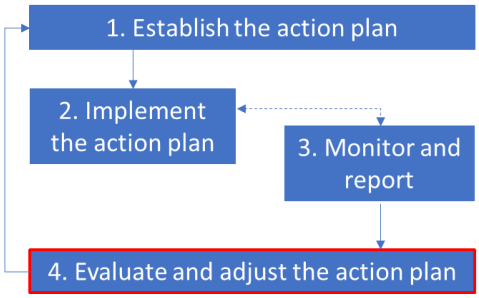
assets, people, organisation, and technology. It would be appropriate to include details of what will in fact be measured in the overall framework for operational risk management. All the information from the indicators should be gathered together in a reporting structure which may be defined by the risk management function. The most important aspect of the reporting is that it is clearly and concisely stated what has been measured and the consequence the indicator may have on the business objectives and activities in the action plan.

The "deliverable" from this third stage in this model for operational risk management will be a documented collection of indicators and conditions which form the basis of both the implementation and evaluation of the action plan.

2.4 Evaluate and adjust the action plan

This stage concerns ensuring a good coordination and communication as to how far the enterprise through its action plan is on the right track in its treatment of operational risk.
The most important success criterion for this stage is that the enterprise should ensure a sound basis for future development by means of the monitoring and reporting in the previous stage.

Put simply this final stage is about ensuring the quality of or re-establishing the action plan. Based on the measurement indicators and reporting made the current situation can be appraised once more. Having re-appraised the current situation a re-assessment should be made of each activity in the action plan to ensure it is still relevant and effective.



The following questions may be used to facilitate an effective evaluation of the activities:

- Has the basis for establishing the action plan changed? In which case, what has changed and what impact should this have on the description of operational risks?
- Are the potential future events that were identified in the risk evaluation still relevant, or should some be removed and replaced with other more relevant scenarios?
- Is the prioritising of potential events or conditions still correct or should something be amended?
- Are the assumptions related to capability of being able to address the prioritied potential future events or conditions still valid?

From this stage there follows a smooth transition back to the first stage because a new profile of status and risks which formed the basis for the original action plan will result in an updated action plan.

About this publication

This document has been prepared by a working group consisting of committed and proficient institute members. IIA Norge (IIA Norway) extends a heartfelt thanks to:

Mazhar Ahmad, Head of operational risk, Statkraft
Alf Olav Uldal, Quality manager, Lede AS
Martin Stevens, Internal auditor, Gjensidige Forsikring
Roger Ølstad, Partner/head of cyber and information security, Agenda Risk AS

Thanks also to Martin Stevens for translating this document to English.

About IIA Norway

The mission of IIA Norway is to provide members with a sound professional foundation and strengthen organisations' knowledge of management, control, and internal audit.

We have established professional and active networks for the sharing of experience and knowledge. We have separate networks, for finance, leaders, public sector, compliance and business ethics, risk management, and IT audit. Each network consists of committed members drawn from various organisations within or across specific industries. As a member of IIA Norway you will have the opportunity to participate in all networks and have access to tools and documentation from the networks. For further information see www.iia.no.

Other relevant Guidelines from IIA Norway available in English are:

- Guidelines for Governance
- Guidelines for the Compliance Function
- Good Practice Guidelines for the Enterprise Risk Management Function
- Maturity model for governance
- Maturity model for risk management
- Questions a board may ask to understand how an organisation controls its risks

IIA Norway also provides further education, leading to the following certification and diplomas:

- Diplomert internrevisor
- Certified Internal Auditor (CIA)
- Certification in Risk Management Assurance (CRMA)