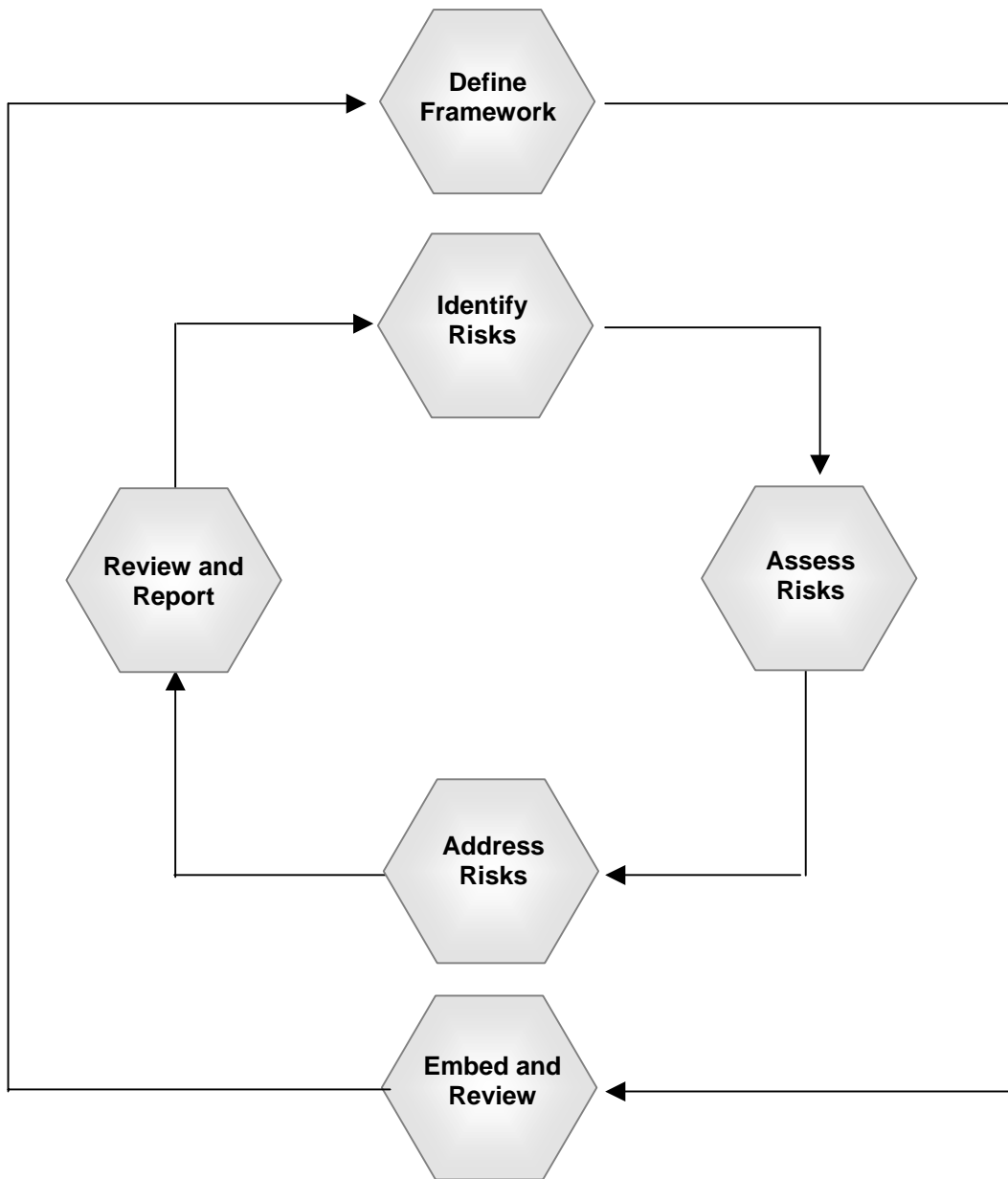


# Introduction to Risk

The task of risk management is to identify risks associated with a particular course of action designed to deliver a particular outcome. Once identified those risks are managed to limit the potential of adverse results and look for positive opportunities.

## Risk Process

Click on a segment for more detailed information.



## Define framework

### Issues covered during this stage

[Define a risk management framework](#)

[What is the context?](#)

[Agree objectives, concerns and constraints](#)

[Agree what constitutes success](#)

[Joint working and partnerships](#)

[Identify the tools and techniques to be adopted](#)

[Decide how impact will be measured](#)

[Decide how probability will be measured](#)

[How the framework supports risk management](#)

[Identify relevant standards, policies and legal requirements](#)

For a wider perspective on establishing and embedding an organisation-wide risk management policy, you are referred to the [Treasury's Orange Book](#), where you will find a high-level risk management model. OGC guidance is focused on the "how-to" processes that underpin effective management of risk and breaks down the generic model into six more detailed stages.

This section therefore deals with establishing a risk policy that can be fitted within the overall corporate business and risk management framework. Whereas it is for the strategic level to determine the degree to which the organisation will balance opportunity and threat (by setting the acceptable level of risk exposure that can be tolerated), individual programmes, projects or operational areas must agree how they will respond to risk within their own specific areas. Part of this policy will be to ensure that risks outside the set tolerance are escalated to a higher authority. The policy will also describe the approach to identifying and evaluating risks, the tools and techniques used to respond and the stakeholders who will be an essential part of the management, reporting and assurance process.

Step 1 of 10 steps

---

#### **What you need to do**

---

Define a risk management framework

---

#### **Points to consider**

---

The aim of this stage is to develop a framework for managing risk based on the risk management policy.

Step 2 of 10 steps.

---

#### **What you need to do**

---

What is the context?

---

**Points to consider**

---

The context of risk management will affect your approach. Consider the following:

- at which level of the organisation is risk management taking place?
  - [strategic](#)
  - [programme](#)
  - [project](#)
  - [operational](#)
- what basic kinds of risk are in prospect?
- what (broadly) will be the consequences of their occurring?
- which [stakeholders](#) are important

Step 3 of 10 steps

---

**What you need to do**

---

Agree objectives, concerns and constraints

---

**Points to consider**

---

Consider what you hope to achieve through risk management, and the constraints upon you.

- what are the aims of risk management in this context?
- what situations do you hope to avoid, preserve or bring about through risk management?
- are there any particular concerns, or specific known risks, that risk management could help with?
- what factors (internal and external) will affect or limit your approach?
- are there any strategies that cannot be applied in your situation?
- what is the corporate risk appetite?

Some of the information appropriate to this stage (such as assumptions or rejected options) should appear in the business case.

Step 4 of 10 steps.

---

**What you need to do**

---

Agree what constitutes success

---

**Points to consider**

---

Ideas of what constitutes successful risk management may differ between stakeholders. You will need to clarify what all stakeholders consider success to be.

Within that, it is important to establish which views of success are more important.

You should also consider how you will demonstrate, to all stakeholders, that success has been achieved.

Additionally, the cost of risk mitigation actions must be considered.

For further guidance, [Treasury's Orange Book](#).

Step 5 of 10 steps.

---

**What you need to do**

---

Joint working and partnerships

---

**Points to consider**

---

Joint working and partnerships often involve more complex types of risk.

For example, if a service (or component of a service) provided by one organisation is delayed or of poor quality, the success of the whole collaboration can be put at risk.

You must make sure that your organisation knows about the risk management approaches of your partners and, where feasible, consider adopting a shared risk register and risk management process.

Sharing information means that the risks of joint working can be identified and managed.

Step 6 of 10 steps.

---

**What you need to do**

---

Identify the tools and techniques to be adopted

---

**Points to consider**

---

Tools and techniques to be adopted will clarify skills required and so reflect resource requirements. These should be realistic for the task in hand.

Techniques to be adopted must be appropriate to support identification and subsequent management and tracking.

Ensuring adequate communications is vital to success.

Step 7 of 10 steps.

---

**What you need to do**

---

Decide how impact will be measured

---

**Points to consider**

---

You need to decide how you will gauge the potential impact of risks. Impact is usually considered in terms of effects in:

- cost
- scheduling
- quality
- scope
- benefits
- risk both individually and as an aggregate

You will need to set tolerances or limits for these areas; for example, how much overspend or delay on a project is deemed acceptable, and how much constitutes an adverse impact.

The ranges should be selected to suit the situation, and also take into consideration the business sensitivity in terms of successful outcome.

The baseline from which impacts are measured could be derived the information set out in documents such as business cases or project plans.

You might decide to use a scale (very low, low, medium, high, very high) to describe the severity of potential impacts. If so, terms must be agreed so that there is consensus on what constitutes (for example) a very severe impact and the measurement scale should be consistent across the organisation.

Step 8 of 10 steps

---

**What you need to do**

---

Decide how probability will be measured

---

**Points to consider**

---

Just as you set scales for the assessment of impact, you will need to decide how the probability or likelihood of risks occurring will be expressed and ensure consistency across different projects and business units.

Probability might be expressed as a percentage or on a less formal scale (very unlikely, unlikely, etc). If a verbal system is used, it is important to clarify between all stakeholders what the commonly accepted meanings of such terms are.

Step 9 of 10 steps.

---

**What you need to do**

---

How the framework supports risk management

---

**Points to consider**

---

The risk management policy needs to be clear and show how management of risk is to be adopted within the situation, and any associated plan (i.e. it should reflect the level, project or programme to which it applies).

The minimum requirements for a [risk management framework](#) are:

- existence of the organisation's risk policy
  - Risk Appetite and capacity
  - Risk Tolerances and thresholds
  - Quality assurance
  - Escalation procedure
  - Risk management strategy
  - Reporting arrangements
  - Early warning indicators
- clear identification of main stakeholders
- clarification of the main approaches to be used to identify; assess and report on risks; as well as look at actions to deal with risks
- clear assignment of responsibilities for managing risk and reporting to senior management, especially risks which cut across core business activities and organisational boundaries
- clear audit trail of decisions to ensure that risk management reflects current good practice, with quality assurance of key decisions as input to audit.

Step 10 of 10 steps.

---

**What you need to do**

---

Identify relevant standards, policies and legal requirements

---

**Points to consider**

---

Your approach must meet legal and regulatory requirements. The aspects that apply will vary depending upon the activity being undertaken. It is vital to meet your organisational needs for corporate governance.

## Identify Risks

## Issues covered during this stage

[Identify the risks](#)

[Gather or update information on possible risks](#)

[Additional points to consider](#)

[Consider opportunities and how these are affected](#)

[Group risks \(initially\) according to where they have been identified](#)

## Synopsis

This section deals with the identification and recording of risks in the risk register. The risk register should be shared with suppliers and partners in delivery. Risks may be divided into 4 categories:

- [Strategic](#)
- [Programme](#)
- [Project](#)
- [Operational](#)

As a general rule, risks should be related to key business objectives (whether these are at an operational, project or programme level).

There are two aspects to risk identification: The initial phase, where a new activity or programme is being initiated and continuous identification due to shifts in environmental factors or other changed circumstances. It is essential that the process is kept alive and that stakeholders are actively involved in raising any new or previously unidentified risks.

Step 1 of 5 steps.

---

**What you need to do**

---

Identify the risks

---

**Points to consider**

---

The purpose of this section is to create and update a risk register or risk log to record the currently identified risks.

Step 2 of 5 steps.

---

**What you need to do**

---

Gather or update information on possible risks

---

**Points to consider**

---

You need to identify risks at all levels in the organisation.

There are different types of risks relevant at each of the four levels:

- Strategic/corporate: commercial, financial, political, environmental, strategic, cultural, acquisition, political and quality risks.
- Programme: Procurement/acquisition, funding, organisational, projects, security, safety, quality and business continuity risks
- Project: Personal, technical, cost, schedule, resource, operational support, quality and provider failure
- Operations: Personal, technical, cost, schedule, resource, operational support, quality, provider failure, environmental and infrastructure failure.

Step 3 of 5 steps.

---

**What you need to do**

---

Additional points to consider

---

**Points to consider**

---

- Subdividing the situation into a set of activities or products will help to make it manageable. Even the most complex situation should not involve more than 35 major activities or products.
- List possible threats for the situation as a whole. Some threats will be more significant than others.
- Identify all the threats. Any threat not identified will lead to a risk that is not being actively managed or monitored and so is, in effect, accepted.
- Consider stakeholder viewpoints as their views on what poses a threat will vary.
- Check that there are realistic plans for how providers could deliver the outcomes sought from the activity; check that there is shared understanding of the risks, whilst recognising that customers' and providers' perspectives on risk will not be the same.
- [Treasury's Orange Book](#) contains a useful summary of the PESTLE model (politics, economic, socio-cultural, technological, legal, environmental) for considering strategic risks.
- Think 'outside the box'

Step 4 of 5 steps.

---

**What you need to do**

---

Consider opportunities and how these are affected

---

**Points to consider**

---

Consider opportunities to support the vision for the future. Each opportunity is likely to have associated risk which must be considered and included in the risk register.

You are on step 5 of 5 steps.

---

**What you need to do**

---

Group risks (initially) according to where they have been identified

---

**Points to consider**

---

Risks that have a similar cause may be able to be managed through adoption of the same response strategy or be owned by the same person (as they may be able to control that aspect).

Similar types of risk may also have interactions that will need to be investigated further in later steps.

## **Assess risks**

### **Issues covered during this stage**

[Identify probable risk owners](#)

[For each threat, identify possible risk owners](#)

[Assess their potential to accept the responsibility](#)

[Consider opportunities and how these are affected](#)

[Update risk register with information on probable risk owners](#)

[Evaluate risks](#)

[Assess qualitatively each of the identified threats in terms of their probability, impact and proximity](#)

[Quantitative risk assessment](#)

[Update Risk Register](#)

[Sort risks in order of priority](#)

[Establish organisation's risk appetite](#)

[Set delegated risk tolerance levels](#)

[Gain agreement and ensure regular review of the risk tolerance level](#)

Update Risk Register

## **Synopsis**

This section deals with the identification of risk owners who are named individuals with the capability, authority and experience to deal with that particular risk. Identified risk owners should be added to the risk register generated earlier.

This section also deals with evaluating identified risks using agreed measures. Typically in a project context, risks may be associated with cost, quality and schedule, but they can also range from a financially quantifiable threat to a more subjective one such as a fall in reputation. Risk can be thought of in terms of probability (likelihood of occurrence), impact (the damage done if it materialises) and proximity (when the risk is expected to arise). Risks can then be prioritised according to business criticality, which is likely to involve a combination of severity of impact, high probability and close proximity. In order to assess the actual level of threat, it is important at an early point to distinguish between inherent risk (the risk before any mitigation) and the residual risk (the level of risk expected to remain after control actions have been applied).

This section also deals with determining the aggregate level of risk that an organisation is prepared to tolerate (the risk appetite); this level may change from time to time or even change for different areas of the business or between major programmes. Once established, the “top-down” risk appetite sets a risk tolerance level that will be used to decide which risks require the most attention and when escalation is needed. It is important to note that some risk is unavoidable or may present a positive opportunity and that residual risks (those remaining after mitigation) may require detailed contingency plans to be in place.

## Obtain commitment from the business

You are on Step 1 of 14 steps.

---

**What you need to do**

---

Identify probable risk owners

---

**Points to consider**

---

The objective of this stage is to identify possible risk owners from within the stakeholder group, for each threat identified so far.

Step 2 of 14 steps.

---

**What you need to do**

---

For each threat, identify possible risk owners

---

**Points to consider**

---

For each threat, identify the person with the best capability, authority and experience to understand and manage the risk that it poses.

Risk owners should all be considered as stakeholders - even if they have only a passive interest in the outcome they will be interested in the area of risk they are managing.

Step 3 of 14 steps.

---

**What you need to do**

---

Assess their potential to accept the responsibility.

Consider opportunities and how these are affected.

---

**Points to consider**

---

Risk owners must have sufficient authority to take on the responsibility for their risks. Assessments of levels of responsibility will be valuable when considering responses to risk.

Consider opportunities to support the vision for the future. Each opportunity is likely to have associated risk which must be considered and included in the risk register.

---

**What you need to do**

---

Update risk register with information on probable risk owners

---

**Points to consider**

---

- Some threats may have several potential owners.
- All practical choices should be documented at this point.

Step 6 of 14 steps.

---

**What you need to do**

---

Evaluate risks

---

**Points to consider**

---

The objectives of this stage are:

- to determine the probability, impact and proximity (timing) of the identified threats
- where appropriate, to sort risks based on their importance (criticality).

Step 7 of 14 steps.

---

**What you need to do**

---

Assess qualitatively (based on the scale decided earlier) each of the identified threats in terms of their probability, impact and proximity.

---

**Points to consider**

---

- The validity of qualitative analysis is directly related to several factors including:
  - the accuracy of historical information
  - the bias and inexperience of personnel
  - ambiguity over the terms of reference for the analysis.

- While it is important to analyse each risk individually, it is also essential to look for dependencies between risks (either threats or impacts).
- Identification and evaluation of technical risks needs to be completed early to ensure that all potential resolution options are opened up. Correcting problems later in the process is generally more costly and difficult.

Step 8 of 14 steps.

---

**What you need to do**

---

Quantitative risk assessment

---

**Points to consider**

---

- You should attempt quantitative (financial) analysis of both the threat itself and the likely cost of mitigating measures in order to inform subsequent decisions.

Step 9 of 14 steps.

---

**What you need to do**

---

Update Risk Register

---

**Points to consider**

---

- All risks should be retained on the Risk Register and monitored to retain control aggregation of risk registers across projects and programmes will allow the organisation to build a risk profile which in turn will aid prioritisation, maintain an audit trail of actions and improve wider monitoring.

Step 10 of 14 steps.

---

**What you need to do**

---

Sort risks in order of priority

---

**Points to consider**

---

Attention will usually focus on the top 5-10 risks, but it is important to reflect on the delivery lifecycle, for example more attention may be paid to commercial risks or risks to benefits at certain stages than at others.”

Step 11 of 14 steps.

---

**What you need to do**

---

Establish organisation's risk appetite

---

**Points to consider**

---

The objective is to determine, first, the aggregate level of risk that the organisation is prepared to tolerate. This will take account of prevailing circumstances and the organisation's culture and strategic goals – for example, there may be distinct drivers for an organisation whose primary role is customer service delivery, as opposed to one more involved in developing policy for others. Other factors that may help formulate the risk appetite include budgetary constraints, the level of political embarrassment deemed acceptable, or dependencies on other initiatives, partners, suppliers or agencies.

Step 12 of 14 steps.

---

**What you need to do**

---

Set delegated risk tolerance levels

---

**Points to consider**

---

The risk appetite can be seen as a series of boundaries authorised by management within which programmes and business units must operate. Innovation or major change activities will probably involve higher levels of risk than would be appropriate for a mission critical area where business continuity is essential.

Once the overall risk tolerance level has been set, decision must be made about the delegated risk tolerance levels for different parts of the business or for major programmes. This will help determine risk prioritisation in those areas and establish trigger points for escalation of individual risks that exceed the agreed level. It will also support better resource allocation, for example, greater effort can be concentrated on addressing risks above the tolerance level whilst resources may be freed up from devoting excess attention to risks that lie within acceptable boundaries.

Finally, mapping risks against agreed tolerances allows sharper decision-making at key points in a project life-cycle ("stop-go" reviews) or at OGC Gateways.

Step 13 of 14 steps.

---

**What you need to do**

---

Gain agreement and ensure regular review of the risk tolerance level

---

**Points to consider**

---

The risk tolerance level is the maximum overall exposure to risk that should be accepted, based on the benefits and costs involved.

If the responses to risk cannot bring the risk exposure to below this level, the activity must be referred upwards and will probably need to be stopped.

Hence the level must be agreed with the appropriate level of management. For example on a project the risk tolerance level will be agreed between the SRO and the Project Manager. The risk tolerance level must be reviewed in the light of changing circumstances and as a result of feedback from projects and at portfolio management level.

Step 14 of 14 steps.

---

**What you need to do**

---

Update Risk Register

---

**Points to consider**

---

- All risks should be retained on the Risk Register and monitored to retain control.

## Address risks

### Issues covered during this stage

[Identify suitable responses to risk](#)

[Identify a range of practical responses to each significant risk on the Risk Register](#)

[Investigate if the responses themselves create an opportunity or pose a threat to other areas of activity and identify these links](#)

[Sort the risks into priority order](#)

[Cross-reference risks to the responses](#)

[Update the Risk Register with this information](#)

[Implement responses](#)

[Analyse the overall exposure to risk against the 'risk tolerance level'](#)

[Select the most appropriate set of responses](#)

[Analyse whether these responses produce additional unintended consequences - if so, further planning is required](#)

[Identify owners for risk threats and responses](#)

[Finalise the plans for activity and any subsequent contingency/business continuity plans](#)

[Update the Risk Register and ensure managers receive appropriate information](#)

[Gain approval to the plans and risk ownership allocation](#)

[Allocate resources to the plans and/or assign responsibilities for risk](#)

## Synopsis

This section deals with ways of responding to threats. Five possible responses are identified and each is looked at in turn. If the decision is taken to “treat” (mitigate) the risk, there are four further possible types of control that can be applied. All of the actions must be recorded in the risk register as new risks or opportunities may emerge as a result of corrective action and “closed” risks may recur as the situation changes.

This section also deals with putting into action the most appropriate responses to all significant risks in order to reduce or maintain overall risk exposure within the tolerance levels agreed by the business. These action plans should be incorporated into normal programme and project plans they are not separate action plans. Resources and responsibilities for actions and risks must be clearly allocated.

Step 1 of 15 steps.

---

### **What you need to do**

---

Identify suitable responses to risk.

---

### **Points to consider**

---

The purpose of this stage is to try and turn risk (uncertainty) to the organisation’s advantage by constraining threats or taking advantage of opportunities that arise in the process of dealing with the risks.

Step 2 of 15 steps.

---

### **What you need to do**

---

Identify a range of practical responses to each significant risk on the Risk Register.

---

### **Points to consider**

---

The top level of options for each risk comprises:

- Tolerate it (because you can live with it, or because the cost associated with dealing with it may be disproportionate – although you may still need to develop a contingency plan).
- Transfer it to the party best placed to manage it (in the case of financial risk this could be through insurance) but note that some business or reputational risks may be difficult to share or transfer in practice.
- Terminate the activity – not necessarily possible in the case of mandated or regulatory measures, but the option of closing down a project or programme where the benefits are in doubt must be a real one.
- Take the opportunity – in addition to the other responses, it may be possible to exploit a new opportunity resulting from mitigation or transfer, or to re-deploy resources freed up from termination.
- Treat the risk – often the preferred option - can be further sub-divided into four types of control:
  - Preventive – these are measures taken before the undesirable outcome can happen, for example a separation of roles ensure actions are overseen and properly authorised;
  - Corrective – applied after the event, these may consist of contractual remedies to recover overpayments or obtain damages or may be a detailed contingency plan that will be triggered by the event (for example, disaster recovery or business continuity plans).
  - Directive – these focus on ensuring the right outcome, for example by insisting on the proper training or enforcing Health and Safety rules.
  - Detective – measures taken after the threat has materialised, for example to learn and apply lessons elsewhere, or a process of reconciliation of financial records or asset inventory

Responses should be proportional to the risks they address. Apart from the most extreme circumstances, it is usually enough to have controls that give a reasonable assurance of confining likely loss to acceptable limits for the organisation, programme, project, or operational environment.

Every response has an associated cost, if the risk should materialise; the response must offer value for money in relation to the risk that it is controlling. In general, the purpose of control is to contain risk rather than remove it.

The risk response process should involve identifying and evaluating a significant range of options for treating risks, and preparing and implementing risk management plans.

Risks that have very high probability and impact must be addressed. Lesser risks may be less critical and some may be accepted as they are.

To minimise the risks associated with service provision, put in place processes that will encourage cooperation and open dialogue between the organisation and its providers. Ensure that providers share information about problems at the earliest opportunity so that small issues do not escalate.

Step 3 of 15 steps.

---

**What you need to do**

---

Investigate if the responses themselves create an opportunity or pose a threat to other areas of activity and identify these links

---

**Points to consider**

---

Step 4 of 15 steps.

---

**What you need to do**

---

Sort the risks into priority order

Cross-reference risks to the responses

Update the Risk Register with this information

Implement responses

---

**Points to consider**

---

The objectives of this stage are to:

- select the most appropriate response to all significant risks
- finalise associated plans and gain approval
- ensure appropriate information on risk is communicated to appropriate management
- implement plans

Step 8 of 15 steps.

---

**What you need to do**

---

Analyse the overall exposure to risk against the 'risk tolerance level'

---

**Points to consider**

---

Consider the current exposure to risk and identify those risks that must be addressed to bring the activity within the identified tolerability level.

Step 9 of 15 steps.

---

**What you need to do**

---

Select the most appropriate set of responses

---

**Points to consider**

---

Your responses to risk should ensure that risk exposure is within toleration and that the actions are within budget. Some risk responses may reduce the overall potential benefits and this loss must be taken into account when deciding on which action to take.

Once selected, responses must have appropriate plans agreed that may affect project or programme plans, or contingency plans.

Step 10 of 15 steps.

---

**What you need to do**

---

Analyse whether these responses produce additional unintended consequences - if so, further planning is required

Identify owners for risk threats and responses

---

**Points to consider**

---

- Allocate responsibility at a senior level for managing key risks.
- Ensure that every risk has an owner; there may be separate owners for the actions to mitigate the risks.
- Ensure anyone allocated ownership has the authority to take on the responsibility and that they are aware that they are the designated owner.
- Adopt a mechanism for reporting issues - ultimately to the individual who has to retain overall responsibility.
- Owners may be identified to be responsible for ensuring risk actions are carried out effectively. The risk owners need to have suitable authority to be given this responsibility.

Step 12 of 15 steps.

---

**What you need to do**

---

Finalise the plans for activity and any subsequent contingency/business continuity plans

---

**Points to consider**

---

- Allocate responsibility at a senior level for managing key risks.
- Ensure that every risk has an owner; there may be separate owners for the actions to mitigate the risks.
- Ensure anyone allocated ownership has the authority to take on the responsibility and that they are aware that they are the designated owner.

- Adopt a mechanism for reporting issues - ultimately to the individual who has to retain overall responsibility.
- Owners may be identified to be responsible for ensuring risk actions are carried out effectively. The risk owners need to have suitable authority to be given this responsibility.

Step 13 of 15 steps.

---

**What you need to do**

---

- Update the Risk Register and ensure managers receive appropriate information
- Gain approval to the plans and risk ownership allocation
- Allocate resources to the plans and/or assign responsibilities for risk

## Review and Report

### Issues covered during this stage

[Gain assurance about the effectiveness of responses](#)

[Gather information about risk responses](#)

[Reassess the exposure to risk and update the Risk Register](#)

[Re-evaluate activity](#)

[Check that risks are still within agreed tolerances and make this information available for external audit/review](#)

## Synopsis

This section deals with determining that the risk responses initiated are having the desired effect, that is, ensuring that the overall exposure to risk remains within the agreed tolerance levels. These measures can be internally or externally audited and/or reviewed.

Step 1 of 5 steps.

---

**What you need to do**

---

Gain assurance about the effectiveness of responses

---

**Points to consider**

---

The objectives of this stage are:

- To determine if the risk response has been implemented
- to monitor risk responses and assess their effectiveness

- to assess that the activity remains within the risk tolerance level
- to determine if the risk response has produced any unintended consequences

See the checklist on risk responses

Step 2 of 5 steps.

---

**What you need to do**

---

Gather information about risk responses

---

**Points to consider**

---

- Responses must be clearly defined so that it is possible to assess their effectiveness. If appropriate measurements cannot be collected the analysis will be limited.
- The emphasis here is on how well risks themselves are identified and managed (not how effective the management of risk processes are).

Step 3 of 5 steps.

---

**What you need to do**

---

Reassess the exposure to risk and update the Risk Register

---

**Points to consider**

---

Step 4 of 5 steps.

---

**What you need to do**

---

Re-evaluate activity

---

**Points to consider**

---

Regular reviews are essential at project and programme level and these must be aligned with corporate processes and procedures. The Risk Implementation Manager is responsible for wider oversight and reporting.

At Programme level, Board members have a duty to probe and challenge risk management in conjunction with corporate and external assurance roles (OGC Gateways, Non-executive Directors, Audit etc).

Step 5 of 5 steps.

---

**What you need to do**

---

Check that risks are still within agreed tolerances and make this information available for external audit/review

---

**Points to consider**

---

The Orange Book provides further guidance on the interfaces between different organisational levels of risk management and how the RIM co-ordinates reporting and adjustment activity.

## Embed and review

### Issues covered during this stage

[Embed and review risk management culture](#)

[Assess application of the management of risk processes](#)

[Review effectiveness of the application and the maturity of the organisation](#)

[Identify areas for change and improvement](#)

[Produce a report on effectiveness and pass to management](#)

### Synopsis

This section deals with ensuring that management of risk is an intrinsic part of the way the organisation works. This may form part of an annual report on the effectiveness of the organisations framework for managing risk. Such reports should highlight things that went well as well as areas and plans for improvement at programme and project level, activity to review and improve risk management must be continuous. A key element of the assurance role will be to check that risks are being proactively identified and managed and that attention given by the Board and other stakeholders reflects the lifecycle stage reached.

You are looking to see if risk management is making a difference:

- can it be shown that outcomes have improved?
- can the benefits be objectively measured?

Step 1 of 5 steps.

---

#### What you need to do

---

### Embed and review risk management culture

---

#### Points to consider

---

The objective of this stage is to produce a report on how well the management of risk processes and framework are embedded into everyday management activities.

You are looking to see if risk management is making a difference:

- can it be shown that outcomes have improved?
- can the benefit be objectively measured?

See [checklist](#)

Step 2 of 5 steps.

---

**What you need to do**

---

Assess application of the management of risk processes

---

**Points to consider**

---

You are looking to see if risk management is an intrinsic part of the way the organisation works and that this is reflected in the risk policy.

Step 3 of 5 steps.

---

**What you need to do**

---

Review effectiveness of the application and the maturity of the organisation.

---

**Points to consider**

---

- As well as assessing if the process is being followed appropriately, consider if the current policy is appropriate for the organisation.
- If new to risk management it will take time for people to adopt the processes/techniques.
- Should the risk policy be updated to support the organisation, either because it did not provide the right level of support, or because the organisation has started to embed risk within the culture and is now ready to take additional elements as the maturity levels increase?

Step 4 of 5 steps.

---

**What you need to do**

---

Identify areas for change and improvement

---

**Points to consider**

---

Everyone with an assurance role must confirm that the risk management process is subject to continuous improvement and that stakeholders are actively involved in communicating and optimising responses to significant risks.

Step 5 of 5 steps.

---

**What you need to do**

---

Produce a report on effectiveness and pass to management.

---

**Points to consider**

---

For projects and programmes, risk activity should form a standing item at Board meetings and should form an integral part of the decision making process. At the strategic level, the Risk Improvement Manager and the Audit Committee may have specific responsibility for providing internal assurance that risk is being managed effectively, while external bodies and supply chain organisations (the Extended Enterprise) may also have a major impact on the way risks are managed.

## Managing risk at the strategic level

### Issues covered during this stage

[Types of risks](#)

[Where to apply risk management](#)

[When to do it](#)

[Who is involved](#)

[Roles and responsibilities](#)

### Synopsis

Management of risk at the strategic level is concerned with setting strategic direction and balancing potential opportunity against the costs and risks. High level appraisals of strategic risks are a major feature of the business case when plans for change are being considered. For example, the organisation may be thinking about innovative ways of delivering business services that involve new technologies. Options for exploiting opportunities for improved performance could be assessed against the risks associated with relatively unproven technologies and/or collaboration with private sector partners.

Step 1 of 4 steps.

---

**What you need to do**

---

Types of risk

---

**Points to consider**

---

At the strategic level the concerns are about where the organisation wants to go, how to get there and how to ensure survival. Any major risks at this level are likely to stop the organisation functioning. Risks at this level are typically concerned with commercial, financial, directional, environmental, cultural, acquisition, political and quality issues.

Programme, project and operational risks should be escalated to this level against set criteria where they exceed agreed tolerances – such as unacceptable exposure to risk, outside certain limits and could affect strategic objectives.

Step 2 of 4 steps.

---

**What you need to do**

---

Where to apply risk management

---

**Points to consider**

---

Corporate / Departmental and programme objectives and goals are being set at this level. Risk management must be carried out in line with the objectives and goals that are initially set at this level. It is normally at this level that the widest context of the business is reviewed – its financial, legislative, political, social, competitive and cultural environments. Without a clear view of the strategic, programme, project and operational objectives and goals, risk analysis and management may be inappropriately applied. If the analysis is severely constrained, the output is likely to be misleading.

Commitments to corporate governance are made at this level. This requires senior management to understand the risks associated with their decisions and actions; there must be the involvement of the management board, especially the Accounting Officer.

Decisions are taken on future strategy and changes to commercial arrangements, which could involve issues relating to the business, technical environment, people, accommodation or the start of a new acquisition lifecycle. Considerations about commercial arrangements include setting the overall approach to working with partners and use of the Private Finance Initiative (PFI).

Step 3 of 4 steps.

---

**What you need to do**

---

When to do it

---

**Points to consider**

---

Risk management, while an intrinsic part of strategic management, should be explicitly applied at specific points in the lifecycle of the business or response to major events. Risk management activities should be triggered when:

- identifying, reviewing, agreeing and setting corporate / departmental objectives and goals
- assessing and choosing options for implementation of strategic initiatives
- formulating, submitting or reviewing feasibility studies/business cases to support future strategies
- testing the underlying assumptions within the business case or proposed strategies
- formally instigating, approving or reviewing programmes, projects and operational activities (including their objectives, goals and performance)
- there is any indication that changes in external factors, such as political, social, economic, regulatory, commercial or financial issues could affect the strategy, mission, objectives and goals
- there have been changes, or potential changes are identified to stakeholder involvement
- an unforeseen event has occurred that could have an impact on the corporate objectives, such as change in regulations
- making key acquisition decisions eg at the start of a new acquisition lifecycle.

Step 4 of 4 steps.

---

**What you need to do**

---

Who is involved

---

**Points to consider**

---

The following table summarises the roles and responsibilities involved in risk management at this level.

Roles and responsibilities	
Who should own and apply the risk process	Responsibilities
Management board, Accounting Officers, Directors. Steering Groups, Stakeholders, SROs	Ownership of the overall risk mgt framework and risk process. Establishing policy on risk and signing off risk strategy, including willingness to take on risk and risk tolerance levels.
Business consultants, Technical strategists	Application of risk process to business changes, such as in strategy, establishment of new programmes
Risk Committee, Audit Committee	Ensuring compliance with corporate/departmental guidance on internal control
Legal, Financial, procurement advisors, Specialist advisors, such as security / business continuity management	Managing legal, commercial, market related risks. Ensure risks are reported to appropriate levels and responses made. Approval of budgets to be allocated to the management of risk

## Managing risk at the programme level

### Issues covered during this stage

[Type of risk](#)

[Where to apply risk management](#)

[When to do it](#)

[Who is involved](#)

[Roles and responsibilities](#)

Step 1 of 4 steps.

---

**What you need to do**

---

Types of risk

---

**Points to consider**

---

At the programme level, managers are responsible for transforming high level strategy into new ways of working to deliver benefits to the organisation. Typical risks at this level are associated with acquisition, funding, organisational and cultural issues, projects, security, safety, quality and business continuity.

Project and operational risks should be escalated to this level against set criteria where they exceed agreed tolerances – such as unacceptable exposure to risk, outside certain limits and could affect programme objectives.

Step 2 of 4 steps.

---

**What you need to do**

---

## Where to apply risk management

---

### Points to consider

---

Risk management at this level should be applied where:

- the information about risk can influence the programme most effectively, such as where critical decisions are to be taken
- decisions being taken at the strategic level require programme risk information
- programme objectives are, or will be influenced by the changes to strategic objectives and vice versa
- where appropriate, Gate/Peer reviews will be required.

Step 3 of 4 steps.

---

### What you need to do

---

When to do it

---

### Points to consider

---

Risk management at this level should be triggered when:

- reviewing and reporting programme status with regard to corporate and programme objectives
- providing formal approval for, or reviewing projects against programme and project objectives, goals and performance
- endeavouring to engage stakeholders in the programme
- conducting programme planning or rescheduling
- key projects show symptoms of failing, or have failed to meet their objectives
- starting a new acquisition lifecycle of a programme
- preparing for Gate/Peer reviews
- significant changes are planned or have occurred at any of the other levels – that is, strategy, project, operations
- they are an integral part of the Programme/project management process, such as PRINCE2®.

Step 4 of 4 steps.

---

### What you need to do

---

Who is involved

---

### Points to consider

---

The following table summarises the roles and responsibilities involved in risk management at this level.

Risk management at the programme level is primarily concerned with the overall direction of the programme and the management of interdependencies (individual projects that make up the programme and the wider business context). Where appropriate, decisions about risk management form an important part of the business case.

Roles and responsibilities
----------------------------

Who should own and apply the risk process	Responsibilities
SROs	Approve funding for programme and project risk management plans
Programme Board	Balancing an acceptable level of programme risk against business opportunity and deciding level of acceptability of individual risks.
Accounting Officers	Categorising and prioritising risks across the various projects including setting or validating tolerance levels for risk at project level
Programme Director and Managers	Ensuring that the design process, technical change control and quality assurance address risk.
Programme Delivery Manager	Approve and sign off project risk management plans and monitor status and effectiveness of process and plans.
Programme Support Office	Escalation of risks to business executive, Accounting Officers, stakeholders and appropriate management boards.
Programme risk specialists, eg.security	Check feasibility of technical risks through appropriate authority
Design Authority Business Change Managers Procurement Managers Contract managers Legal, regulatory advisors	Advise and provide guidance to projects on project risk within the context of the programme and relevant strategy.

## Managing risk at the project level

### Issues covered during this stage

[Types of risk](#)

[Where to apply risk management](#)

[When to do it](#)

[Who is involved](#)

[Roles and responsibilities](#)

## Synopsis

Risk management at the project level focuses on keeping unwanted outcomes to the minimum. Decisions about risk management at this level form an important part of the business case; where providers and/or partners are involved you must gain a shared view of the risks and how they will be managed.

Risk management at the project level is a major theme in the Cabinet Office report Successful IT: Modernising Government in Action.

Experience of projects involving IT-enabled change highlights the need for management of project risk outside the immediate concerns of the project:

*An appreciation of business risk management at all levels in an organisation will help ensure the impact of a project is fully understood and monitored throughout its life. In particular, procedures designed to improve reporting and the upward referral of problems are needed.*

Step 1 of 4 steps.

---

### What you need to do

---

Types of risk

---

### Points to consider

---

Risks at the project level typically include personal, technical, cost, schedule, resource, operational support, quality and supplier failure issues. Operational issues will also need to be considered where they are relevant to the outcomes of the project.

Strategic and programme related risks should be communicated to this level where they could affect project objectives. Risks relating to individual projects should be communicated to other projects and operations where appropriate.

Step 2 of 4 steps.

---

### What you need to do

---

Where to apply risk management

---

### Points to consider

---

Risk management at the project level should be applied where:

- project objectives and goal are being assessed
- project initiation is being carried as part of the project lifecycle and when using the Project Profile Model (PPM)

Step 3 of 4 steps.

---

**What you need to do**

---

When to do it

---

**Points to consider**

---

Risk management at the project level should be triggered when:

- there is a change in the project lifecycle, e.g., each major phase, stage and decision point of the project and as part of the project planning process
- major acquisitions are being made as part of the project.
- re-assessing project benefits and the business case
- preparing to handing over from a development environment to operations
- any significant changes are notified to the project, e.g., re-organisation, change of supplier, unforeseen changes to other interdependencies such as connected projects or programmes
- re-visiting the cost benefit and risk case behind the project or programme.
- preparing for Gate/Peer reviews

Step 4 of 4 steps.

---

**What you need to do**

---

Who is involved

---

**Points to consider**

---

The following table summarises the roles and responsibilities involved in risk management at this level.

Roles and responsibilities	
Who should own and apply the risk process	Responsibilities
Project Boards SROs Project Sponsors	Balancing an acceptable level of project risk against programme and project objectives and business opportunity
Project Managers	Implementing the risk management process to be used at Project Level
Project Support Office Project Risk Specialists	Ensuring interdependency related risks are reported and addressed

Programme Director and Managers	Ensuring that the design process, technical change control and quality assurance address risk.
Project Delivery Managers	Escalation of risks to programme level and operations where required and responding to risks notified to the project
Project Work Groups/teams support the risk Business Continuity/Security Managers	Allocation of project resources to process
Project auditors	Approval of funding for project risk related activities

## Managing risk at the operational level

### Issues covered during this stage

[Types of risk](#)

[Where to apply risk management](#)

[When to do it](#)

[Who is involved](#)

[Roles and responsibilities](#)

### Synopsis

Risk management at the operational level is primarily concerned with continuity of business services. You may have providers who are carrying out risk management relating to your services. However, you must be aware that you cannot transfer risk totally; ensure that your own risks are managed. There should be a shared understanding and agreement on the risks and their management.

Step 1 of 4 steps.

---

**What you need to do**

---

Types of risk

---

**Points to consider**

---

Risks at the operational level typically include personal risks; technical, cost, schedule, resource, operational support, quality, provider failure and environmental issues; and infrastructure failure. All the higher levels have input to this level; specific concerns include business continuity management, contingency planning, support for business processes and customer relations.

Step 2 of 4 steps.

---

**What you need to do**

---

Where to apply risk management

---

**Points to consider**

---

Risk management at this level should be applied where:

- projects are going to be delivered into an operational environment and will impose either a significant change, or a potential risk on the operational environment – for example:
  - the deliverables are of inadequate quality
  - timescales for delivery impose constraints upon the operational environment being ready. The operational environments often have different drivers and owners to projects that can often result in serious conflict if their objectives and goals are not synchronised. Operational people need allow for and schedule in the impact of changes such as caused by projects
- changes in the operational environment could significantly undermine the project, programme and strategic objectives if the risks are not understood and communicated
- there is a requirement to identify the critical business process and technology
- there is a need for internal control from a corporate governance perspective – for example, an IT project that delivers a system with poor information security controls or no business continuity strategy could create a corporate governance problem
- there are regulatory and legal constraints, such as health and safety, data protection and information.

Step 3 of 4 steps.

---

**What you need to do**

---

When to do it

---

**Points to consider**

---

Risk management at this level should be triggered when:

- considering undertaking significant commitments on behalf of the organisation – for example, changing providers or starting new contracts, major new acquisitions
- establishing a new operational process or considering any significant change to the existing operational environment – for example, relocation, downsizing, significant maintenance shutdowns
- major investment decisions are being made
- identifying future human resource requirements for operational staff
- there is a perceived unexpected threat to the operational environment, eg environmental issues, demonstrations
- any unforeseen event has occurred that could threaten 'business as usual'.

Step 4 of 4 steps.

---

**What you need to do**

---

Who is involved

---

**Points to consider**

---

The table below summarises the roles and responsibilities involved in risk management at this level.

Roles and responsibilities	
Who should own and apply the risk process	Responsibilities
IT Directors/Managers Business managers	Balancing an acceptable level of operational risk against programme and project objectives and business opportunity
Finance Director / Accounting Officer	Implementing the risk process to be used at the operational level
Information Security Manager Operational support staff	Ensuring interdependency related risks at the operational level are reported and addressed
Business Continuity Manager	Escalation of risks to strategic, programme and project level where required
Health and Safety Officer	Allocation of resources to support the risk process
Facilities Manager Human Resource Managers Legal and regulatory officers Practitioners supporting the process, eg information security, business continuity, software engineers, Auditors	Approval of funding for operational risk activities

## Stakeholder issues (stakeholder map)

### Purpose:

To document all parties (individuals or groups) who have an interest in the outcome of the proposed activity. This may include individuals or groups outside the business. The interests of each stakeholder are identified and the map is used to ensure all interests are catered for, which includes keeping them informed and accepting feedback.

The Stakeholder Map is output from the culmination of work undertaken on stakeholder analysis. A stakeholder is anyone affected by a decision and interested in its outcome. This can include individuals or groups, both inside and outside the organisation. The stakeholder analysis is a piece of work undertaken to assess the influence and importance of each individual stakeholder or stakeholder group. The Stakeholder Map is typically shown as a matrix,

detailing individual stakeholders or groups of stakeholders and their particular interests, along with the communication route and frequency for each stakeholder or group of stakeholders.

### **Fitness for purpose checklist:**

- Have all the stakeholders and their interests been identified?
- Is there agreement from all interested parties about the content, frequency and method?
- Has a common standard been considered?
- Has time to carry out the identified communications been allowed for in the stage plans?

### **Notes:**

It is important to determine the interests of all stakeholders, who may represent different customer groups, and to resolve conflicting requirements. The Cabinet Office is developing guidance on customer focus, one of the Prime Minister's four principles of reform.

### **Suggested content:**

Typically a Stakeholder Map will include as a minimum:

List of stakeholders

List of interests (i.e. the issues that concern them, their attitude towards aspects of the situation that present a risk, and the extent to which they can influence the way that the risk is addressed)

Matrix of stakeholders to interest and the relative importance of the project/magnitude of the risks to each.

### **Further information:**

See [Introduction to Programmes](#)

See also the document outlines for [Communication strategy](#)

[Managing Successful Programmes](#)

## **Risk Management Policy**

### **Purpose:**

The risk management policy is to communicate how risk management will be implemented throughout an organisation (or part of an organisation) to support the realisation of its strategic objectives.

## Composition

Typically a policy will include:

- Introduction
- Risk appetite and capacity
- Risk tolerance thresholds
- Procedure for escalation
- Roles and responsibilities
- Glossary of terms
- Risk management process
- Early warning indicators
- Tools and techniques to support the process
- When risk management should be implemented
- Reporting
- Budget
- Quality assurance
- Annual review

## Fitness for purpose checklist:

- Is the policy clearly stated?
- Is it clear who, within the organisation, is responsible for the policy?
- Is it clear how the policy will be implemented?
- What is the timetable for implementation?
- Has best practice guidance been incorporated in the new policy?
- How is the policy to be communicated throughout the organisation?
- Is it clear who is affected by the policy?
- Are all people employed by the organisation affected by the policy or is it just a discrete group?
- Do partners and suppliers have to comply with the policy?
- Is it clear what is required by the individuals in order to comply with the policy?
- Is it clear what management structures are required to facilitate implementation, use and monitoring of the policy?
- Is it clear what review process will be undertaken to ensure the policy is working?

## Notes:

### Policies and standards

Policies and standards ensure that processes, procedures and deliverables are consistent and meet the needs of the business, while complying with current legislation. Some policies, such as equal opportunities, will also be partners and suppliers.

Example topics for policies and standards:

- Enabling policies are those that aim to support, promote and encourage the deployment of effective information systems processes and services.
- Restraining policies are those that aim to control or constrain the activities in the various parts of the organisation.

Examples of areas where you may need to introduce enabling policies are:

- Central provision and allocation of resources, such as equipment, technical staff, software and services
- Arrangements with suppliers, procurement procedures and contractual terms
- The role of providers in the provision of support and training, and user documentation
- The provision of common services, such as generic application systems to meet common requirements, to all parts of the organisation
- Procedures for prioritisation of developments, the planning of a phased introduction of facilities to the organisation, and the implementation of pilot projects where relevant
- The use of external services, such as consultants, database services and maintenance services
- Policies for provision and monitoring of ergonomic aspects of IT systems, including the user interface
- Procedures for system implementation and project management, such as use of the PRINCE methodology.

Examples of areas where you may need to introduce restraining policies are:

- Requirements for compatibility and conformance with standards and guide lines on selection and use of software and document formats
- Definition of procedures for disaster recovery, system security and systems audit
- Standards and procedures for identifying, validating, storing and accessing shared information at work-group, business function or corporate level
- Operating procedures for users of desktop facilities, including policies on local purchase and import of software, and exchange of data media
- Procedures for on-line and off-line document storage, naming, retention, purging and archiving.

Information management - policy topics include:

- Information and data ownership and sharing
- EDM/ERM
- Knowledge Management
- External communication
- Security
- Interoperability
- Business continuity
- Publications policy
- Policies for access, media, preservation/archive; audit

Security – policy document to include:

- a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing
- a statement of management intent, supporting the goals and principles of information security
- a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organisation
- a definition of general and specific responsibilities for information security management, including reporting security incidents
- references to documentation which may support the policy.

## Source information:

[Vision statement](#)

[Programme plan](#)

## Further information:

See the briefing on [governance](#).

## Risk management framework

### Purpose:

To define how management of risk will be handled within the associated context (could be organisation-wide or for a specific activity such as a project). It covers the lifetime of the activity. It provides information on roles, responsibilities, processes and procedures, standards, tools, facilities and documentation to be produced. It sets the context in which risks are managed, in terms of how they will be identified, analysed, controlled, monitored and reviewed. It must be consistent and comprehensive with processes that are embedded in everyday management.

### Fitness for purpose content:

- Does the framework identify relevant standards, policies and legal requirements?
- Does the framework identify (or validate) the context and perspective for the situation (e.g. strategic, operational? Which stakeholders' views are of primary importance?)?
- Are the stated management of risk objectives, constraints and concerns agreed (or validated)?
- Has the framework established how a successful outcome is to be judged?
- Does the framework identify the tools and techniques to be adopted?
- Does the framework identify the scale for evaluation of risk?

### Suggested content:

It addresses how:

- risks are identified
- information about their probability and potential impact is obtained
- they are quantified, taking into account expert advice and the degree of uncertainty
- options to deal with them are identified, taking into account constraints, such as internal obligations

- decisions on risk management are made. This includes the criteria used to decide when further risk reduction is necessary, taking into account costs and benefits
- these decisions are implemented. This includes the principles guiding the choice of how to intervene (such as education, information, inspection) and on whom to target any intervention
- actions are evaluated for their effectiveness
- appropriate communication mechanisms are set up and supported
- stakeholders are engaged throughout the process - especially suppliers and partners.

## Source information:

[Business Case](#)

[Programme Plan](#)

[Project Plan](#)

[Project Brief](#)

[Project Initiation Documentation](#)

## Notes:

Where partners and/or suppliers are involved, it is essential to have shared understanding of risks and agreed plans for managing them.

There are four broad types of risk -

## Strategic Risk

The strategic perspective maintains a view of executive-level decision-making relative to the organisation's external environment and to other organisations that work with or against it.

Strategic risks are those risks concerned with ensuring overall business success, vitality and viability. Materialisation of a strategic risk will be perceivable externally by owners, investors or funders, and will affect the reputation of the organisation.

Strategic opportunities and threats are generally identified:

- Through escalation of risks from programme, project, or operational activities
- As a by-product of corporate and business planning activities
- By partner organisations that share interests with the organisation.

## Programme Risk

The programme perspective maintains a view of a significant change to the organisation relative to other changes and relative to the ongoing operations of the organisation.

Programme risks are those risks concerned with transforming business strategy into new ways of working that deliver measurable benefits to the organisation. Stakeholders with an interest in the programme benefits will become aware of the appearance of programme risks.

Programme opportunities and threats are generally identified:

- Through the escalation of risks from projects within the programme
- During programme start-up
- By other programmes with dependencies or interdependencies with this programme
- By operational units affected by the programme.

## Project Risk

The project perspective maintains a view of successfully delivering a predefined output or product and, as a consequence, enabling the delivery of business benefits to the organisation.

Project risks are those risks concerned with delivering defined outputs to an appropriate level of quality within agreed time, cost and scope constraints. The recipients of project outputs will identify the appearance of project risks that will affect the time, cost, quality or scope of outputs.

Project opportunities and threats are generally identified:

- Through the escalation of risks identified when delivering work packages
- During project initiation
- By other projects within a common programme or other projects within the organisation
- By the project's customers and suppliers.

## Operational risk

The operational perspective maintains a view of the people, processes, and technologies that support ongoing business-as-usual or service delivery activities of the organisation in relation to customer expectations. In this context, services may be delivered to internal customers (e.g. by a human resources function) or to external customers (e.g. financial management services by a money management firm). The operational perspective also monitors how strategic changes to the organisation affect ongoing business-as-usual and service delivery activities.

Operational risks are those concerned with maintaining an appropriate level of business service to existing and new customers. Customers receiving the affected business service will recognise the appearance of operational risks.

Operational opportunities and threats are generally identified:

- Through the escalation of risks from business or service delivery teams (e.g. engineering, information systems, finance, human resources, security, fraud, customer support, etc.)
- By service-enabling suppliers
- By service-receiving customers.

## Further information:

See the briefing for [Risk management strategy](#) and [Risk Management Framework](#).

[Management of Risk](#): Practitioner guidance

## Healthcheck: How well is your organisation managing risk?

NOTE: This checklist can be used from different perspectives such as:

- before, or during [Gateway Reviews](#)
- when preparing for, or carrying out internal and external risk audits
- when considering a new initiative, such as a major project, entering a new acquisition lifecycle
- when progress reporting to HM Treasury
- when preparing to raise commitment to improving the existing process.

## Key elements

Elements needed for an effective management of risk process and the indicators of a successful process include:

- policies for the management of risk and the benefits of effective risk management are clearly communicated to staff
- senior management support, promote, own and lead on risk management
- there is an organisational culture that supports well thought-through risk taking and innovation
- management of risk is fully embedded in the management process of the organisation, including the associated controls and distribution of management information
- the identification and assessment of risk is aimed at actively managing the key risks to the achievement of objectives
- the risks posed by working with other organisations are assessed.

## Review of overall effectiveness

- Is management of risk implemented across the organisation to all line management and business management, as well as project and programme management?
- Is there a formal documented policy for the management of risk? Does the policy address the following:
  - the corporate view of risk management?
  - processes and procedures?

- the desired benefits to be achieved?
  - roles and responsibilities?
  - facilities/tools required?
  - documentation standards?
- Is the management of risk policy regularly reviewed?
- Are business continuity and contingency plans in place in the event that risks result in adverse consequences?
  - Are these plans tested (regularly reviewed and re-tested)?
  - Are those responsible aware of their roles with regard to each plan?
  - Is there a clearly identified authority to make the decision to implement the plan?
  - Are copies of the plan held off-site? (and still accessible in an emergency?)
- Is there increasing visibility of risk and appropriate communication to staff so they understand their responsibility for being alert to risks?
  - Are staff being trained or receiving guidance in risk management?
  - Are risks being raised to the appropriate level?
  - Are major risks assigned owners?
  - Are you applying existing approaches/practices to address risk problems?
  - Are you following the standard processes and procedure for addressing problems in managing risk?
- Is there clear identification of types/categories of risk?
- Are risk evaluation criteria clearly identified and articulated?
  - Are risk responsibilities assigned for reporting and managing identified risks?
  - Is the effectiveness of risk treatments monitored and reviewed?
  - Is there appropriate communication and consultation with others within your organisation and with stakeholders?
- Is the risk documentation appropriate?
  - Is the documentation consistent throughout?
- Where appropriate, are you following the risk profile model in accordance with Cabinet Office guidelines?
- Is risk management ongoing and integrated with other procedures?