**[Programme/ Project Name]**

Risk Management Strategy

[Month YYYY]

Contents

[Purpose 2](#_Toc520884371)

[Glossary 3](#_Toc520884372)

[Roles and responsibilities 4](#_Toc520884373)

[Risk Management Process 6](#_Toc520884374)

[Communication and engagement 8](#_Toc520884375)

[Techniques 9](#_Toc520884376)

[Benefits Management Interface 10](#_Toc520884377)

[Early warning indicators 11](#_Toc520884378)

[Risk management activities and escalation 12](#_Toc520884379)

[Information flows 13](#_Toc520884380)

[Review of Risk 14](#_Toc520884381)

[Annex A – RAID Log 15](#_Toc520884382)

[ 15](#_Toc520884383)

[Annex B – Risk Severity 16](#_Toc520884384)

[Annex C - Impact & Likelihood rating scales 17](#_Toc520884385)

[Annex D – Project and Programme Impact Rating Scales 18](#_Toc520884386)

[Annex E – Risk Response Strategies 19](#_Toc520884387)

**The practical Guidance contained within is intended to assist with putting risk, issues and opportunity management into practice and assist in the development of a programme risk strategy. Italic text is for reference only.**

# Purpose

*[Give a brief description of your programme/project]*

Start text here.

Effective risk management is critical to project success – it can save time, improve quality and reduce the cost of achieving an agreed outcome. Effective management of risk also allows for the maximising of opportunities.

This strategy details the approach to risk management that the *[programme name]* will use.

*[Identify the nature and level of risk acceptable within the programme]*

Start text here.

# Glossary

|  |  |
| --- | --- |
| Term | Definition |
| Impact | The effect or influence that a risk or issue may exert on a Programme’s goals. For risks this is expressed in terms of schedule and cost, expressed quantitatively, or qualitatively as very high, high, medium, low or very low |
| Likelihood | Something currently happening that is having a negative impact on the Programme cost, timescale or achievement of deliverables and requires resolution for the Programme to proceed successfully. Issues can arise from a risk that has occurred or any other event that were not predicted. |
| Opportunity | An uncertain event or set of circumstances that, should it occur, will have a positive effect on the achievement of a Programme’s objectives |
| Probability Impact Grid | Risk scoring table combining the assessments of probability and impact to ascertain a comparative risk score |
| Programme Risk / Opportunity | Any risk or opportunity that is managed at the level of the Programme |
| Risk | An uncertain event or set of circumstances that, should it occur, will have an adverse effect on the achievement of the Programme’s objectives |
| Risk Analysis | Structured examination of the constitution of risks affecting a Programme, to gain an understanding of their individual significance and their individual and combined influences upon the Programme’s objectives. Risk analysis covers both cost and schedule exposure |
| Risk Exposure | Is the statistically derived aggregate financial cost to the Programme, at any given time, of all identified risks. This exposure is determined using probabilistic method (Monte Carlo Simulation) |
| RAID Log | A RAID log is a programme management tool to track **risks**, **actions**, **issues**, **decisions and Assumptions**. It is a document that is constantly maintained throughout the project/program.The risk log records information such as cause, effect, impact, likelihood, mitigations, owner, for things that could go wrong but have not yet occurred. The actions log records information such as owner, due date, action progress, for things that need to be done. The issues log records information such as issue description, owner, mitigation, for known problems that have occurred (if a risk triggers, it becomes an issue as well). The decision long records information such as decision description, date, owner for key decisions to be made in the project/program. |

# Roles and responsibilities

Roles and responsibilities for managing risk within [programme/project name] are detailed below. The table shows the roles and a description of their responsibilities in the management of risk.

|  |  |
| --- | --- |
| Role | Description |
| Senior responsible owner | The single individual with overall responsibility for ensuring that the Programme/Project meets its objectives and delivers the stated benefits. The SRO is therefore accountable for ensuring that the exposure of the programme/project to risk is manageable and that .all Programme and project risks are identified and being managed effectively. The SRO has ownership and accountability of the overall Risks Management Policy. This includes ensuring that a policy on risk is established and signing off the Risk Management Policy, in so doing accepting the willingness to take risks to the identified tolerance levels. |
| Programme director | Accountable to the SRO for the delivery aspects of the programme and management of senior stakeholders. Provides leadership, direction and authority within and across the Project. |
| Project manager | The project manager of an individual project is responsible for managing risk within the defined scope of that project. This includes ensuring that team members follow the risks management processes, that risk management is integral to the way the project operates and that all reporting is clear, honest, open and complete. Project managers are responsible for determining which project risks should be escalated. |
| Risk owner | Member of the programme/project team who is responsible for the effective management of an individual risk, including establishing the risk severity, developing an appropriate mitigation plan and ensuring that mitigation actions are completed in a timely manner. The Risk Owner is responsible for alerting the project/programme manager of changes to the profile of the risk as and when they occur. |
| Risk actionee | Responsible for the implementation of risk response actions, taking direction from the risk owner and providing support. |
| Risk and issue manager (RIM) | Responsible for developing and operating the risk management process. The RIM is the custodian of the programme risk log, and is responsible for the production of risk management reports as required by the Programme management team and governance bodies. The RIM is responsible for working with the programme managers to ensure that they understand the tools and techniques available to them to manage risk, and assist project managers by identifying opportunities for improvement. |
| Project team members | Responsible for identifying risks and bringing them to the attention of the Project Manager, carrying out any mitigation actions as assigned by the Risk Owner, and reporting status of these actions to the Risk Owner. |

# Risk Management Process

This process complements the Home Office Risk Management Policy and Guidance and is based upon the Infrastructure and Project Authority Managing Successful Programmes Best Practice Guidance. Those responsible for risk management should also be familiar with the [Home Office Risk Management Policy & Guidance](https://horizon.fcos.gsi.gov.uk/file-wrapper/home-office-risk-management-policy-and-guidance).



**The Risk Management Cycle**

* **Identification** Risks shall be identified in the light of the programme’s objectives and scope, the assumptions that have been made, who the stakeholders are, where the programme fits inside the organization and the current environment. Threats to the programmes objectives as well as opportunities to overachieve on outcomes and benefits shall be classified as risks and entered in the risk section of the RAID log.

The risks identified will be described in the best possible way to ensure they are fully understood by the entire Programme team. In order to separate risks from their causes and effects, a three-part structured Risk Statement shall be used. A clear description of a risk will follow the guide below:

* **Cause** “Due to …” - identifying the factual set of circumstances that a risk is based on
* **Effect** “there is a risk that …” - describing the event or series of events (uncertain outcome) that constitute the risk
* **Impact** “resulting in …” - identifying the impacts / consequence of the risk occurring on the Programme objectives

It is a requirement that each risk has a Risk Owner to ensure that even the smallest risk is being monitored at some level by a Programme Team Member. The Risk Owner is defined as the person on the Programme, or supporting the Programme, who is best qualified to understand and manage the risk.

*[The risk log forms part of the RAID log and can be found at Annex A.]*

* **Assessment** The threats and the opportunities of risks will be estimated in terms of their probability, impact and proximity. At programme level, the net aggregated effect of the identified threats and opportunities on the programme shall be estimated to help to form a view of the aggregated level of risk that the programme is facing as it progresses. Scales for estimating likelihood and impact, giving the criteria to be used for each level within the scale can be found at [Annex C](#_Annex_C_-) and [Annex D](#_Annex_D_–).

Within the Home Office, a five-point scale is used when assigning a rating to both the likelihood and impact of individual risks (very high, high, medium, low, and very low). The Table at [Annex B](#_/Annex_B_–) provides a summary mapping of these. [Home Office Risk Management Policy & Guidance](https://horizon.fcos.gsi.gov.uk/file-wrapper/home-office-risk-management-policy-and-guidance) provides more detail. Having scored likelihood and impact you should determine an overall risk-rating, based on the matrix and enter it in the risk log.

* **Proximity** reflects the fact that risks will occur at particular times in the future and the expected value will vary according to when they occur. Understanding of a risk’s probability and impact informs management of the priority of a risk, understanding of a risk’s proximity informs management of its impending urgency. Knowing the proximity also helps to identify the appropriate response and the required trigger and timing of the response. Proximity is assessed as Black – within a month; Red one to three months; Amber - three to six months; Green – Six months to a year and is entered in the risk log.
* **Plan** For each risk that has been identified and appropriately assessed, the programme shall develop (and record in the risk log) a series of responses available that it can use individually or in combination to deflect a threat or help to realize an opportunity. [Annex E](#_Annex_E_–) details potential responses.
* **Implement**  The planned risk management actions are implemented and monitored as to their effectiveness, and corrective action is taken where responses do not match expectations. Clear roles and responsibilities shall be allocated, to ensure that responsibility for the management and control of the risk, and for the implementation of response actions are clearly allocated.

*[Risks should be managed as a coherent whole, these being identified, assessed and controlled at the appropriate (Project, Workstream, Portfolio) level, being escalated for information or action, as appropriate. This also involves prioritising them in order of severity, so that effort can be focussed on those most likely to materialise and which will have the greatest impact.]*

# Communication and engagement

Risks and opportunities will be communicated throughout the Programme organisation by using the RAID log, regular risk reviews / workshops and reports. The Programme RAID log and associated reports will be stored in a central location to ensure that that all Programme team members have visibility of the major risks, opportunities and mitigations.

It will be the responsibility of the Risk Management Team to develop and encourage a culture of proactive risk management within the Programme team. This will be done through:

* **Engagement.** Ensuring everyone on the Programme understands their responsibilities and are actively engaged in the process
* **Enabling decision making** Ensuring that where decisions are required, they are taken to the Governance Board with decision making authority
* **Common terminology** Utilising a common language throughout the Programme when talking about risk

# Techniques

*[List techniques particular to the programme]*

Start text here.

The Programme team will use the techniques to identify risks:

* Brainstorming/Risk Workshops (Guidance for running risk workshops can be found in the HO Project Delivery Framework)
* Lessons learnt
* Progress reports and governance board meetings
* Ad-hoc identification by Programme Team Member / Stakeholder

# Benefits Management Interface

*[Explain the interface to the benefits management arrangements]*

Start text here.

# Early warning indicators

Particular attention will be paid to:

* Requests to change key programme information
* Reduction or delays in the delivery of expected/planned benefits on time and on budget
* Increase in the level of aggregated risk resulting from project and operational risks
* Changes to organizational structures
* Changes to services or products
* Changes to processes.

# Risk management activities and escalation

*[Detail risk management activities – at least monthly reviews at programme board level]*

Start text here.

As a guideline the following reasons are valid for escalating risks:

* **Ability to Manage** Risk cannot be owned or managed at the current level
* **Conflict Resolution** If there is a disagreement the risk may be escalated to resolve disagreement over who is responsible to resolve, to deal with slow or non-progress of mitigation by another party, or resolve disagreement over ownership
* **Awareness** The next level need to be made aware of the risk because of the urgency to mitigate the; risk, size or range of impacts, in order to flag assumptions or higher management visibility in considered prudent
* **Commonality** Those risks which are common across multiple projects or Risk logs

The decision to escalate should be made at programme board level.

# Information flows

*[Detail risk reporting and escalation. Include the need to report programme risks up the business as usual line. It’s important to be clear the type and frequency of the flows of information in the risk process. This should include:*

* *The process and frequency that risks will be reported to the risk manager.*
* *Sharing of risk logs with PPD on a monthly basis*
* *Any reports that will be produced. Their regularity and their purpose.*
* *The flow of information in and out from the risk manager as well as clear escalation routes.]*

Start text here.

##

# Review of Risk

Risk will be reviewed monthly with attention being paid to:

* Ensuring each risk / opportunity has a dedicated owner
* Identifying response plans with agreed owners and dates
* Verifying that response plans are current and being progressed
* Validating fallback plans and associated trigger dates (risk target dates)
* Reviewing / validating escalated risks and opportunities
* Ensuring the Risk log is populated with all appropriate risks / opportunities

Reviewing a risk will include an assessment of the overall status of the risk. A risk will be closed if either:

* The risk can no longer occur, or is deemed to have no impact if it does materialise. This may be due to the time period where the risk could impact expiring; response actions successfully reducing the likelihood to 0% or all impacts to nil; or a change in the programme resulting in it no longer being relevant; and
* The risk has impacted or the likelihood of the risk occurring has increased to the extent that it should be treated as an issue. In both instances the risk will be closed on the Risk log and transferred to the Issue log where it will continue to be managed.

## Annex A – RAID Log

##

### Risk

A risk is any specific event which might occur and thus have a negative impact on your project or program. Each risk will have an associated likelihood of occurrence along with an impact on your project if it does materialize.

### Actions

The actions, whatever they are, need to be charted. That is noted the date they are completed. During project meetings, refer to this list and check off those actions that have been completed to make sure there’s been follow through.

Actions require an owner. Having an owner makes sure that the action is managed and will not fall through the cracks of a busy project.

### Issues

An issue is anything which arises on your project which you have to deal with in order to ensure your project runs smoothly. An issue is a risk that has materialised, unlike risks which might turn into issues in the future. Details of such risks should be transferred to the Issue management tab of the RAID log.

### Decisions

This is a list of decisions that need to be made over the course of the project. It is a way to collect the thought process of the project, a record of what decisions were made, who made them and why.

### Assumptions

An assumption is something we set as true to enable us to proceed with our project or program. Typically this happens during the planning and estimation phase of the project. As an example of an assumption, during the early planning phase, we might assume that we have access to 10 skilled specialists throughout the duration of the project. By making this assumption it enables us to produce our plan. If this assumption turns out to be false then the project is negatively impacted, because assumptions can turn out to be false and impact your project adversely.

## Home Office Risk MatrixAnnex B – Risk Severity

## Annex C - Impact & Likelihood rating scales

### Likelihood scales

|  |  |  |
| --- | --- | --- |
| **RATING**  | **LIKELIHOOD**  | **DEFINITION**  |
| **VERY LIKELY** or VERY HIGH  | More than 80% chance of occurring.  | **Strategic** ‘Clear and present danger’ represented by this risk – will probably impact on this initiative – sooner rather than later. **Programme/Project** Is likely to happen in the life-cycle of the project, probably early on and, perhaps, more than once. **Operational** The threat is likely to happen almost every day.  |
| **LIKELY** or HIGH  | 51 – 80% likelihood of risk materialising.  | **Strategic** Likely to happen at some point during the next one to two years. **Programme/Project** Likely to happen in the life of the programme or project. **Operational** May well happen on a weekly basis.  |
| **POSSIBLE** or MEDIUM  | 21 – 50% chance of occurring.  | **Strategic** May well occur during the lifetime of the strategy. **Programme/Project** May occur during the life of the programme or project. **Operational** May happen on a monthly basis.  |
| **UNLIKELY** orLOW  | 6% - 20% chance of happening.  | **Strategic** Only small chance of occurring in the lifetime of a strategy. **Programme/Project** Not likely to occur during the lifecycle of the project or programme. **Operational** Does not happen often – once every six months.  |
| **REMOTE** orVERY LOW  | Less than 5% chance of the risk occurring.  | Extremely infrequent – unlikely to happen in a strategic environment or occur during a project or programmes lifecycle. May occur once a year or so in an operational environment.  |

## Annex D – Project and Programme Impact Rating Scales

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RATING  | PUBLIC PROTECTION  | FINANCIAL  | REPUTATIONAL  | DELIVERY AND ACHIEVEMENT OF OBJECTIVES  |
| CRITICAL orVERY HIGH  | A systemic failure for which HO/HO agencies are ultimately responsible exposes the public to serious harm in cases when mitigation was expected.  | - Unfunded pressures greater than £25m. - Fraud, corruption and serious irregularity at ministerial/board level.  | Incompetence / maladministration or other event that will destroy public trust or a key relationship.  | Failure to deliver the majority of HO key objectives (Structural Reform Plan Actions + PM/Home Sec priorities + manifesto pledges/100 days).  |
| SIGNIFICANT orHIGH  | A systemic failure for which HO/HO agencies are ultimately responsible exposes more than 100 people to harm in cases when mitigation was expected.  | - Unfunded pressures greater than £10 million. - Fraud, corruption and serious irregularity at director level.  | Incompetence / maladministration that will undermine public trust or a key relationship for a sustained period or at a critical moment.  | Failure to deliver more than one ‘key’ objective.  |
| MAJOR orMEDIUM  | A systemic failure for which HO/HO agencies are ultimately responsible exposes less than 100 people to harm in cases when mitigation was expected.  | - Unfunded pressures greater than £5 million. - Fraud, corruption and serious irregularity at SCS level.  | Incompetence / maladministration or other event that will undermine public trust or a key relationship for a short period. (e.g. policy u-turn) | Failure to deliver one key objective.  |
| MODERATE or LOW   | A systemic failure which results in inadequate protection individuals/individual communities, including failure to resolve celebrity cases.  | - Unfunded pressures greater than £2 million. - Fraud, corruption and serious irregularity at middle-manager (G7/G6) level.  | Event that may lead to widespread public criticism.  | One of more key objective is only just delivered (e.g. significant delay, or on a downward trend).  |
| MINOR or VERY LOW  | A systemic failure which fails to address lower level harms such as anti-social behaviour.  | - Unfunded pressures under £2 million. - Fraud, corruption and serious irregularity at more junior levels.  | Event that will lead to public criticism by external stakeholders as anticipated.  | No risk to HO demonstrating achievement of its ‘key’ objectives (to time, on budget etc). Failure to deliver more than one group/directorate level objective.  |

## Annex E – Risk Response Strategies

| **Action** | **Response Plan** |
| --- | --- |
| **Transfer** | A third party takes on responsibility for an aspect of the threat by - Insurance: when a premium is paid to an insurance company, the contract indemnifies the insured against the associated financial costs of any loss.Self – insurance: When the cost of the loss is borne by the organisation, for example by setting aside reserves or funds to meet the cost of the loss.Insurance captive: A captive insurance company is one formed to participate in the insurance portfolio of its parent organisation.Contractual transfer: When the financial consequence of the threat is transferred to a third party by means of appropriate clauses in a contract. |
| **Terminate** | This approach involves risk elimination. This can be done by altering an inherently risky process or practice to remove the risk. The same can be used when reviewing practices and processes in all areas of the business. If an item presents a risk and can be changed or removed without it materially affecting the business, then removing the risk should be the first option considered; rather than attempting the treat, tolerate or transfer it. |
| **Tolerate** | No action is taken to mitigate or reduce a risk. This may be because the cost of instituting risk reduction or mitigation activity is not cost-effective or the risks of impact are at so low that they are deemed acceptable to the business.  Even when these risks are tolerated they should be monitored because future changes may make it no longer tolerable |
| **Treat** | controlling risk through actions that reduce the likelihood of the risk occurring or minimize its impact prior to its occurrence.  Also, there are contingent measures that can be developed to reduce the impact of an event once it has occurred |

Home Office Project Delivery Framework (insert link when available)

Portfolio and Project Delivery Directorate

[Knowledge Hub](https://khub.net/web/guest/welcome?p_p_state=normal&p_p_mode=view&refererPlid=47727240&saveLastPath=false&_com_liferay_login_web_portlet_LoginPortlet_mvcRenderCommandName=%2Flogin%2Flogin&p_p_id=com_liferay_login_web_portlet_LoginPortlet&p_p_lifecycle=0&_com_liferay_login_web_portlet_LoginPortlet_redirect=%2Fweb%2Fgovernment-project-delivery-community-hub)

[Home Office Risk Management Policy](https://horizon.fcos.gsi.gov.uk/file-wrapper/home-office-risk-management-policy-and-guidance)