Risk Management Process

< Project Name > Insync Supply Chain Management

Document Control

Changes History

Issue Number	Date	Author	Change

Authorised by

Role	Name	Signed	Date

Distribution

Name	Organisation

Contents

Purpose

The purpose of this document is to define the process for the management of risk within the company. It is intended that this process dovetails into the risk processes of other areas of the company, into the overall risk process and into the risk processes of third party suppliers.

The process is based on, and should be used in conjunction with the Programmes Risk Management Strategy. The Strategy provides an overview of risk management within programmes and will provide useful background detail.

The process will provide the definition of the procedures and controls put in place to identify, analyse and manage risk throughout the nominated Programmes and their projects.

This process is owned by the Programme Support Office (PSO).

Assumptions

Single Central Risk Register

The process assumes that there will be a single central Programme Risk Register.

A single central risk register is fundamental to the process to provide a comprehensive repository of all identified programme and project risks in a standard format together with the results of analysis, proposed actions and status. All risks will be quantified using standard criteria (Probability, Impact, and Proximity etc.) and a single register will enable a high level view of the overall exposure to risk plus the ability to drill down to a specific project or to a single specific risk.

The contents of the manual Programme Risk Register are included in Appendix 1.

Reporting

- PSO will manually produce extracts from the central Programme Risk Register for all Management Board and Programme Board meetings.
- PSO will also provide bespoke reports from the information available in the central Risk Register when requested.

Definition of Risk

Risk can be defined as the chance of exposure to the adverse consequences of future events or more simply as the uncertainty of outcome (whether positive opportunity or negative threat).

The task of risk management is to ensure the organisation makes cost-effective use of a risk process that has a series of well-defined steps to support better decision-making through good understanding of the risks and their likely impact.

Scope

All risks identified within, or relating to, the Programmes and associated projects are within scope. This includes:

- Risks that are managed at Project level either by the Project Manager, a member of the Project Board or a designated project specialist.
- Risks that are escalated to Programme Board level and managed either by the Programme Manager, a member of the Board or a designated agent.
- Risks that are escalated to Management Board level and managed by a member of the Board or a designated agent.

The scope does not include:

- Risks that apply to and are managed at the Operational level.
- Risks that a Management Board escalates to the company.
- Risks that pertain solely to the operations of third party suppliers.
- In all these cases, it is assumed that such risks will be managed under the appropriate local process.

This process covers the management of risk to:

- Record and categorise identified risks in a consistent standardised format.
- Maintain reliable up to date information about each risk.
- Facilitate the monitoring, reporting and escalation of risks to enable efficient decision-making processes

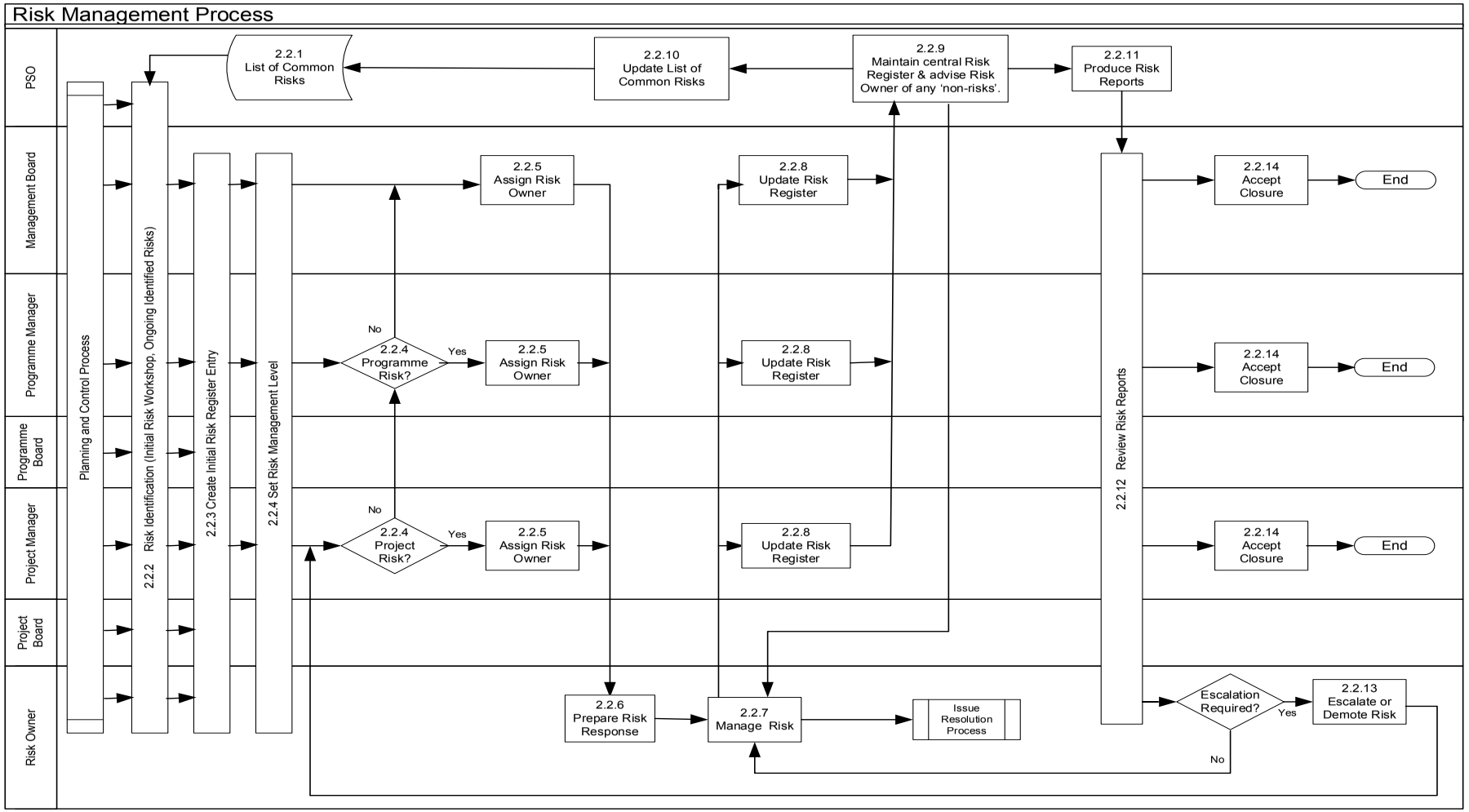
Intended Audience

The process is intended for all individuals who work on, or have involvement in, Programmes and associated project work. Including, but not limited to:

- Programme Managers
- Project Managers
- Project Teams
- Internal and external Auditors
- Quality Control and Assurance

Risk Management Process

Risk Management Process Flow Diagram


Risk Management Process
PSO
Management Board
Programme Manager
Programme Board
Project Manager
Project Board
Risk Owner
Planning and Control Process
2.2.2 Risk Identification (Initial Risk Workshop, Ongoing Identified Risks)
2.2.3 Create Initial Risk Register Entry
2.2.4 Set Risk Management Level
2.2.1 List of Common Risks
2.2.10 Update List of Common Risks
2.2.9 Maintain central Risk Register & advise Risk Owner of any 'non-risks'.
2.2.11 Produce Risk Reports
2.2.5 Assign Risk Owner
2.2.8 Update Risk Register
2.2.14 Accept Closure
End
No
2.2.4 Programme Risk?
Yes
2.2.5 Assign Risk Owner
2.2.8 Update Risk Register
2.2.14 Accept Closure
End
No
2.2.4 Project Risk?
Yes
2.2.5 Assign Risk Owner
2.2.8 Update Risk Register
2.2.14 Accept Closure
End
2.2.12 Review Risk Reports
2.2.6 Prepare Risk Response
2.2.7 Manage Risk
Issue Resolution Process
Escalation Required?
Yes
2.2.13 Escalate or Demote Risk
No

Process Steps

List of Common Risks

The PSO maintains a list of common risks extracted from those recorded in the central Programme Risk Register.

Risk Identification

Risk Workshop

Where practicable, new projects will hold an initial risk workshop during the initiation phase. This will be facilitated by the Project Manager or the Programme Manager and the attendees should include a cross section of stakeholders in the project or programme. Where a risk workshop is not practicable the Project Manager is responsible for the production of an initial project risk log.

Risk workshops can be held at any time throughout the project lifecycle and should at least be considered at every major checkpoint, for example before commencement of each stage or when preparing for OGC Gateway Reviews.

Ongoing Identified Risks

Risk management must be embedded at all levels within the programme or project. As the programme or project progresses new risks may arise at any time.

Whenever a potential new risk is identified it must be raised with the appropriate Project or Programme Manager for review and acceptance into the Programme Risk Register.

Create Initial Risk Register Entry

Risks can be identified and recorded at any level within a programme:

- The Project Manager is responsible for the identification and recording of risks at project level.
- The Programme Manager is responsible for the identification and recording of risks at programme level.
- The Management Board is responsible for the identification and recording of risks at higher levels.

As programmes and projects progress, and new risks are identified, the appropriate level manager is responsible for the ensuring their inclusion in the central Risk Register so that a comprehensive up to date view of risk exposure is maintained at all points throughout the life of the programme or project.

Risks should be recorded locally using Programme Risk Register Template. The appropriate Programme or Project manager is responsible for the creation and maintenance of the register for their area, service or project.

An initial entry will comprise of the following fields:

- Strand/Programme
- Project/Study Name
- Project/Study Number
- Project ID
- Risk Number
- Raised by
- Date Raised
- Risk Status
- Description of Risk
- Impact Description
- Date of Last Update

The content of these fields is explained in Appendix 1 – Risk Register Contents.

Set Risk Management Level

Each risk will be assigned an appropriate management level of Project, Programme Board or Management Board (see Appendix 2 - Guidance on Setting Risk Management Level and Escalation).

This is recorded in the Current Level field of the Register (see Appendix 1 – Risk Register Contents).

Project Level Risks

The Project Manager is responsible for the review of all risks initially assigned for management at project level, ensuring that each identified risk is within the scope and resolution capabilities of the that level. If the risk does not fit within the project level, the Project Manager is responsible for the escalation to the next higher management level to agree the appropriate management level for the risk.

Programme Board Level Risks

The Programme Manager is responsible for the review of all risks initially assigned for management at programme board level, ensuring that each identified risk is within the scope and resolution capabilities of that level. If the risk does not fit within this level, the Programme Manager is responsible for the demotion of the risk to project management level or the escalation to the next higher management level to agree the appropriate management level for the risk.

Management Board Level Risks

The relevant Management Board is responsible for the review of all risks initially assigned for management at board level, ensuring that each identified risk is within the scope and resolution capabilities of that level. If the risk does not fit within the board level, the Management Board is responsible for the demotion of the risk to programme board level or the escalation to the next higher management level to agree the appropriate management level for the risk.

Assign Risk Owner

Once a risk is at the appropriate management level it can be assigned to a Risk Owner who will be accountable for the management of that particular risk.

- The Project Manager will assign Risk Owners for project level risks
- The Programme Manager will assign Risk Owners at programme board level
- The Management Board will assign Risk Owners for higher-level risks

Risk ownership may transfer as treatment of the risk progresses (see Appendix 2 - Guidance on Setting Risk Management Level and Escalation).

Prepare Risk Response

The assigned Risk Owner will review the risk and prepare an appropriate response. This will involve the steps described below and will provide the values for the remaining Risk Register fields (See Appendix 1 – Risk Register Contents).

Probability, Impact & Proximity

The initial step will be to assess and rank the risk in terms of its Probability and Impact (see Appendix 3 - Guidance on Setting Probability, Impact and Proximity). The Risk Appetite (see **Note** below) set for the project or programme will also influence the Probability and Impact levels that are assigned.

Note: Risk Appetite is the amount of risk that the project or programme is prepared to tolerate (be exposed to) at any point in time. This will vary between different programmes and projects and must be clearly defined within each Project Initiation Document (PID).

Proximity is used to indicate the potential future timing of a risk. This will influence the ranking of risks, as those that are immediate will rank higher (and hence need earlier treatment) than those that won't arise until some future date. (see Appendix 3 - Guidance on Setting Probability, Impact and Proximity).

RAG Status

When Probability, Impact and Proximity have been set the Risk Register template will automatically calculate a RAG Status for the risk. This uses a single matrix for the evaluation of all risks, thereby providing a consistent ranking of risk across all Programmes and their projects (see Appendix 4 – Guidance on RAG Status).

Actions

When a risk has been ranked the appropriate response can be defined in line with its level within the overall ranking. Those risks with RAG status of Red will require the most immediate action, with the timeframe easing as lower ranked risks are addressed.

Appendix 5 – MOR Definition of Risks and Responses provides a description of the four standard types of response to risk.

Following all appropriate consultation, the Risk Owner is responsible for the recording the Actions in the Risk Register (see Appendix 1 – Risk Register Contents).

Action Owner, Action Status and Action Target Date

Once the Action is known it can be assigned to an appropriate Action Owner. This may be, but is not necessarily, the same individual as the Risk Owner. If the Action Owner is a separate individual then they will only be responsible for the specific action assigned and will report progress back to the Risk Owner. The Risk Owner retains ultimate responsibility for the risk at all times and manages it through to eventual completion.

Action Status will be used to record the status of the action and its progress towards completion and Action Target Date will be used to record the date for completion of the action (see Appendix 1 – Risk Register Contents).

Manage Risk

The Risk Owner will manage the assigned risk and monitor all associated actions taken to address the risk. The Risk Owner is responsible for the gathering of updates from the Action Owner.

At risk management progresses it may become apparent that a risk needs to be escalated to either somebody of a more senior status or higher level within the Risk Management Process. In such cases, the Risk Owner will initiate escalation to the next level. Similarly, a risk may be demoted to a lower management level if desired.

If a risk becomes reality, the Risk Owner is responsible for the transfer of the entry to the appropriate level within the Issue Register (see Programmes Issue Resolution Process).

Update Risk Register

The Project or Programme Manager is responsible for:

- The maintenance of the Risk Register for their area, service or project.
- The gathering of updates from the various Risk Owners.
- The updating of the status of each risk and its associated actions on a regular basis through to eventual closure.
- The transmission of updated information to the PSO.

Maintain central Risk Register

On a receipt of each update, PSO will transcribe any new entries and all updates to existing entries into central Programme Risk Register.

PSO will review all new entries to ensure that they document genuine risks and to help stop unnecessary time being spent on 'non-risks'. PSO will inform the designated Risk Owner of any questionable entry, and the reasons, so that a decision can be made on its treatment.

Update List of Common Risks

As part of the Risk Register review, PSO will identify any new candidates for addition to the List of Common Risks.

Produce Risk Reports

Risks will feature in all project and programme reports at all levels. All Project Highlight Reports will feature a summary of current risks on the project.

The PSO will produce any regular standard control reports deemed to be required and any specific bespoke reports required by Project or Programme Managers, Management Boards, Programme Boards or Project Boards.

Review Risk Reports

Each level of the programme and project governance should review the status of risks. Regular standard reports will be produced by the PSO for Programme Boards and Management Boards so that they are able to review the status of relevant risks.

A final overview of any risks left open at the point of implementation will be conducted as part of any Post Project Review. The purpose of this final review is to: -

- Identify those risks that, although not fully treated during the life of the project, relate solely to the development process and can be discounted post implementation.
- Identify those risks that could still impact the application(s) and/or process(es) delivered at implementation. These will need to be allowed for or treated during the ongoing support and maintenance post-implementation.
- Document any relevant findings concerning risks identified and actions adopted during the project. This documentation will assist in the risk management of subsequent projects.

Escalate or Demote Risk

As risk reports are reviewed it may become apparent that a risk needs to be escalated to either somebody of a more senior status or a higher level within the Risk Management Process. Alternatively, a risk may be demoted to a lower management level if desired. In such cases, the review body will initiate escalation or demotion by the Risk Owner to the appropriate level (see Appendix 2 Guidance on Setting Risk Level and Escalation).

Accept Risk Closure

As part of the risk report review, the appropriate level manager will review and accept all risks closed during the report period. If there is any debate during this process the manager will liaise directly with the Risk Owner.

Appendix 1 – Risk Register Contents

The following table shows the fields in use within the Excel spreadsheet version of the central Programme Risk Register maintained by PSO and gives an explanation of their content and usage,

Field	Description
Strand / Programme	The owning Strand or Programme
Project/Study Name	Name of the Project/Study at risk
Project/Study Number	Reference Number for the Project/Study at risk
Project ID	The Project ID for the Project/Study at Risk (format Pnnnn).
Risk Number	Unique identifier, allocated sequentially.
Raised by	Name of individual who raised the risk.
Date Raised	Date on which the risk was raised (format dd/mm/yy).
Risk Status	The status of the register entry, one of: **OPEN** **CLOSED** **TRANSFER TO ISSUE**
RAG Status	Current RAG status of the actual risk, **RED**, **AMBER** or **GREEN**. Automatically determined from the **RAG MATRIX** using a combination of Probability, Impact and Proximity.
Probability	The likelihood of the risk being realised, one of: VERY LOW LOW

	MEDIUM HIGH VERY HIGH
Impact	The effect that the realisation of the risk would have, one of: VERY LOW LOW MEDIUM HIGH VERY HIGH
Proximity	A date to indicate the potential timing of the risk (format dd/mm/yy or mmm-yy), i.e. whether the risk is immediate or likely to occur at some point in the future. If the risk is immediate then leave blank. If the risk will occur at some future point enter the future date. The date may change throughout the life of the risk as circumstances change. This date, along with Probability and Impact, will be used to determine the RAG Status.
Description of Risk	This must be clearly stated in terms of cause and effect along the lines of 'There is a risk of/that……..which may result in…….' Also include reference to any Risk Triggers, i.e. if the risk will only manifest itself, or will grow stronger, due to some future event or circumstance then details should be recorded..
Impact Description	A more comprehensive description of Impact if this is required.
Current Level	The CURRENT management level for the risk, one of: BOARD = (Board level) PROGRAMME = (Strand/Programme Level)

	PROJECT = (Project Manager or within project)
Risk Owner	Name of individual responsible for managing the risk.
Action(s)	A list of possible and selected action(s) to be taken in response to the Risk. This field must be completed at Creation even if the only known action at that time is to further analyse the risk to determine possible responses.
Action Owner	Name(s) of individual(s) responsible for implementing action(s).
Action Status	A succinct description of the current progress towards completion of action(s).
Date of Last Update	Date on which the risk entry was last updated.
Action Target Date	Target date for completion of Chosen Action (format dd/mm/yy).
Issue Number	To maintain an audit trail to the Issue Register. -If the risk originated as an Issue then record the original Issue Number. -If the risk is transferred to the Issue Register then record the resulting Issue Number.
Contingency Cost	Cost likely or agreed to be incurred in meeting any mitigating action or contingency. Status of the cost to be noted in the Action Status field.
Closure Date	The date on which the risk is CLOSED or TRANSFER TO ISSUE (format dd/mm/yy).

Appendix 2 – Guidance on Setting Risk Management Level and Escalation

A2.1 Setting Risk Management Level

The management level of the risk should be shown in the "Current Level" field of the Risk Register. This shows the management level deemed appropriate for the risk at the current time

Movement between management levels will depend on the prevailing view of the risk, for example:

- Preventative action could be taken on a risk initially targeted at a high level resulting in a decision to demote the risk to a lower management level
- A risk initially targeted at a low level could, due to subsequent analysis or changed circumstances, increase to such an extent that management of the risk is escalated to a higher level

The process for determining the appropriate management level is as follows:

Level	Decision Process
Management Board	Risks usually managed at this level relate to: Commercial Financial Political Environmental Directional Cultural Acquisition Quality Additionally, when Programme or Project risks exceed the set criteria they are escalated to this level.
Programme	Risks usually managed at this level relate to:

Level	Decision Process
	Procurement/acquisition Funding Organisational Projects Security Safety Quality Business Continuity Additionally, when Project risks exceed set criteria they are escalated to this level. Risks will be escalated from this level if there is evidence that they may affect is wider than the individual Programme or where they exceed criteria set by the relevant Management Board.
Project	Risks usually handled at this level relate to: People Technical Cost Schedule Resource Operational support Quality Provider failure Risks will be escalated from this level if there is evidence that the effect is wider than the individual project, or where they exceed criteria set by the for the project.

A2.2 Risk Escalation

Risks should be considered for escalation to the next appropriate management level where;

- Any risk is identified where management is considered to be outside the scope or capability of the level at which is first reported.
- A risk within a project's scope or authority is deemed likely to affect other projects within the owning programme.
- A risk within a project's scope or authority exceeds agreed limits of tolerance and/or is deemed likely to impact on the objectives of the owning programme.
- A risk within a programme's scope or authority is deemed likely to affect other programmes.
- A risk within a programme's scope or authority exceeds agreed limits of tolerance and/or is deemed likely to impact on the overall strategic objectives of the organisation

In all cases where a risk cannot be managed at the level that it has been reported or assigned to, the Risk Owner will escalate the risk to the appropriate Project Board or Programme Board. The Project or Programme Board will determine whether it is appropriate to escalate ownership to a higher management team.

The Risk Register entry must be updated with the escalation and the action must be supported by a written record within the relevant section of the next progress report (see 'Reporting Process and Schedule').

The new Risk Owner must be satisfied that there has been a Project or Programme Board review process before taking ownership for the risk.

Appendix 3 – Guidance on Setting Probability, Impact and Proximity

A3.1 Probability

Use the Criteria in the table below to assess the likelihood of a risk being realised and assign the Probability shown for that level. The three types of Criteria shown are just different ways of expressing the same level of likelihood.

Probability	Criteria		
VERY LOW	Virtually impossible	< 5% likelihood	Odds > 20/1
LOW	Low but not impossible	5% to 20% likelihood	Odds 20/1 to 5/1
MEDIUM	Fairly likely	21% to 50% likelihood	Odds 5/1 to 2/1
HIGH	More likely than not	51% to 80% likelihood	Odds 2/1 to 4/5
VERY HIGH	Virtually certain	> 80% likelihood	Odds < 4/5

A3.2 Impact

Impact on an activity is usually considered in terms of the effect on cost, scheduling and quality. Each of these will need to be understood in terms of its importance to the activity.

Once relative importance is understood, use the Criteria in the table below to assess the effect of a risk being realised and assign the Impact shown for that level.

Impact	Budget Criteria	Schedule Criteria	Quality Criteria
VERY LOW	Negligible effect on cost, < 3%	Negligible effect on schedule, < 3%	System will fully meet mandatory requirements.
LOW	Small increase in cost, 3 to 10%	Small schedule slip, 3 to 10%	A few shortfalls in desirable functionality
MEDIUM	Significant increase in cost, 10 to 30%	Significant schedule slip, 10 to 30%	Minor shortfalls in one or more key requirements
HIGH	Large increase in cost, 30 to 75%	Large slip in schedule, 30 to 50%	Major shortfall in one or more key requirements
VERY HIGH	Major increase in cost, > 75%	Major slip in schedule, > 50%	Major shortfall in any of the critical requirements

The highest level of Impact should be quoted as the Impact of the Risk. For example, if a Risk scores as “Very High” on Budget Criteria but “Low” on Schedule Criteria, the Impact should be quoted as “Very High”.

A3.3 Proximity

Proximity reflects the timing of the risk.

If the risk is immediate then there is no need to specify Proximity. However, if a risk will only arise at some future date or as a result of some future event then a future date will be recorded.

For instance, if a parallel development or operational upgrade is intending to implement changes prior to the end of a project then there may be a risk that the changes will impact the project. However, the changes may not be implemented or may be implemented only in areas that do not affect the project or may be piloted then rolled out when all risks are eliminated. Any potential risk to the project will only arise as the changes are implemented so the Proximity should be given the date of the intended implementation and the risk should be re-evaluated in the light of new knowledge gained as the date approaches.

Appendix 4 – Guidance on RAG Status

The Programme Risk Register spreadsheet will determine a Red, Amber or Green Status for each Register entry by evaluating the combination of Probability/Impact/Proximity. As Proximity draws nearer to the current date, the Risk Tolerance will lower creating an automatic escalation of the RAG Status.

The tables below show how the three dimensions will be interpreted to determine RAG Status.

Table 1 – Proximity less than 1 month

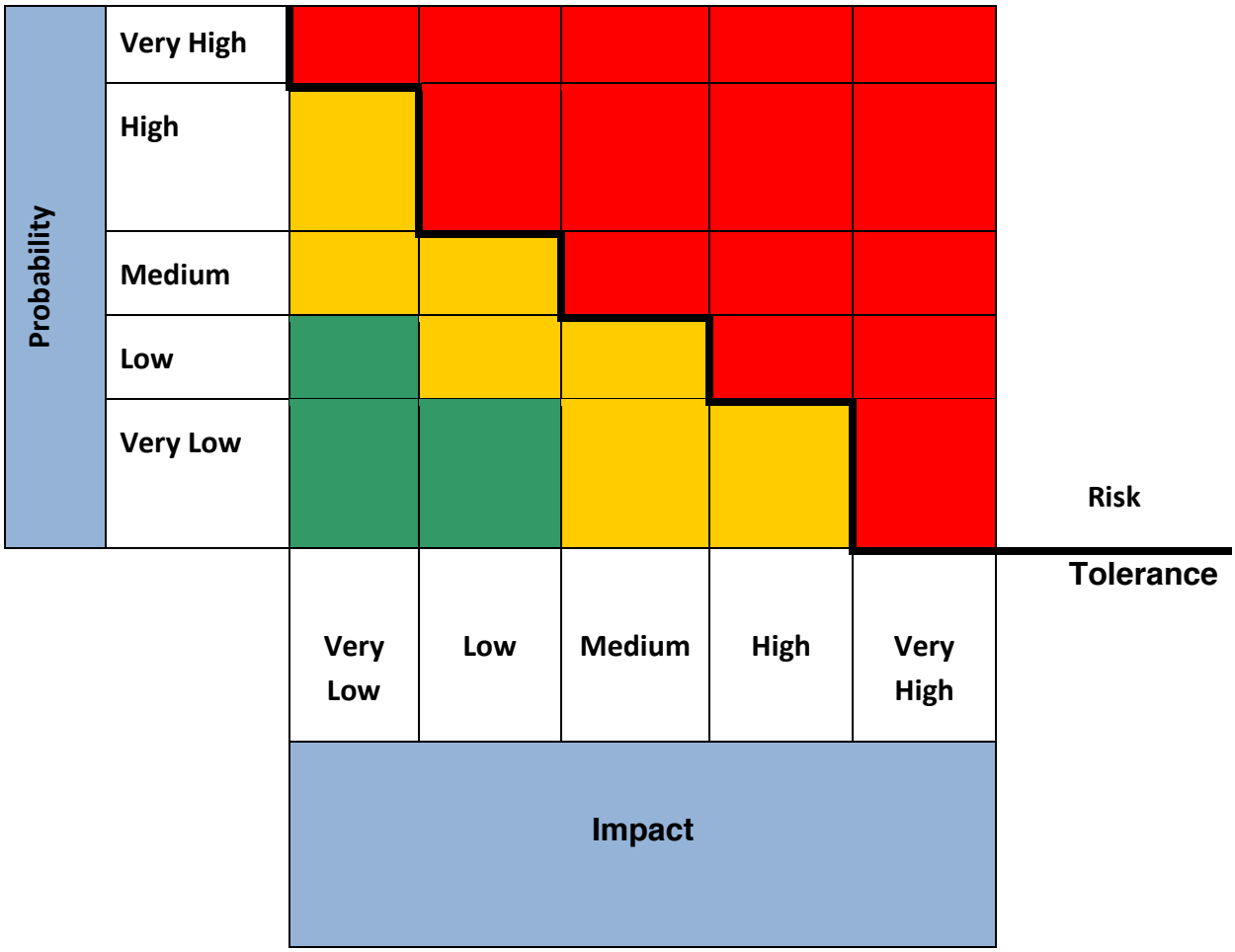


Table 2 – Proximity within 1 to 3 months

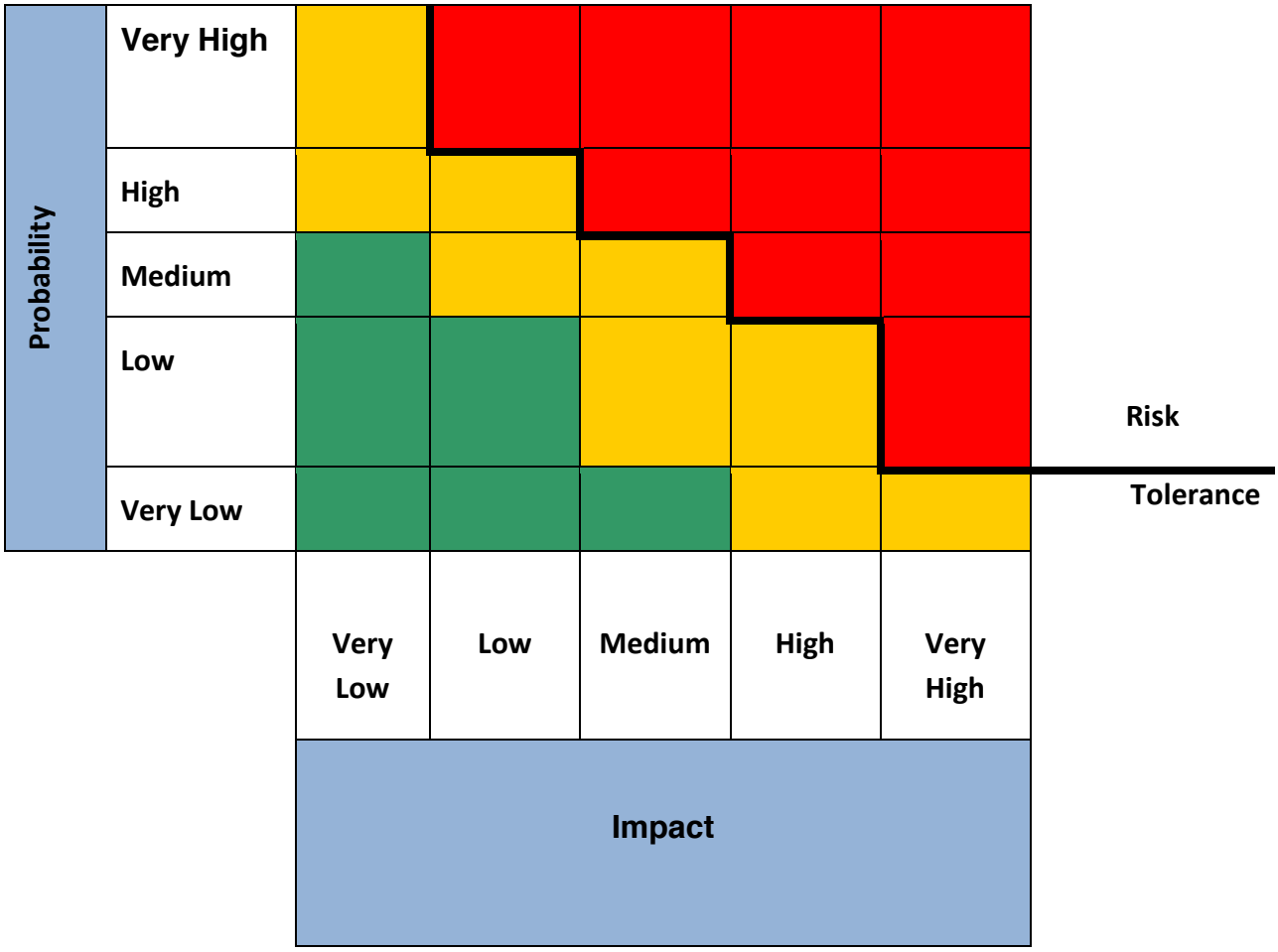
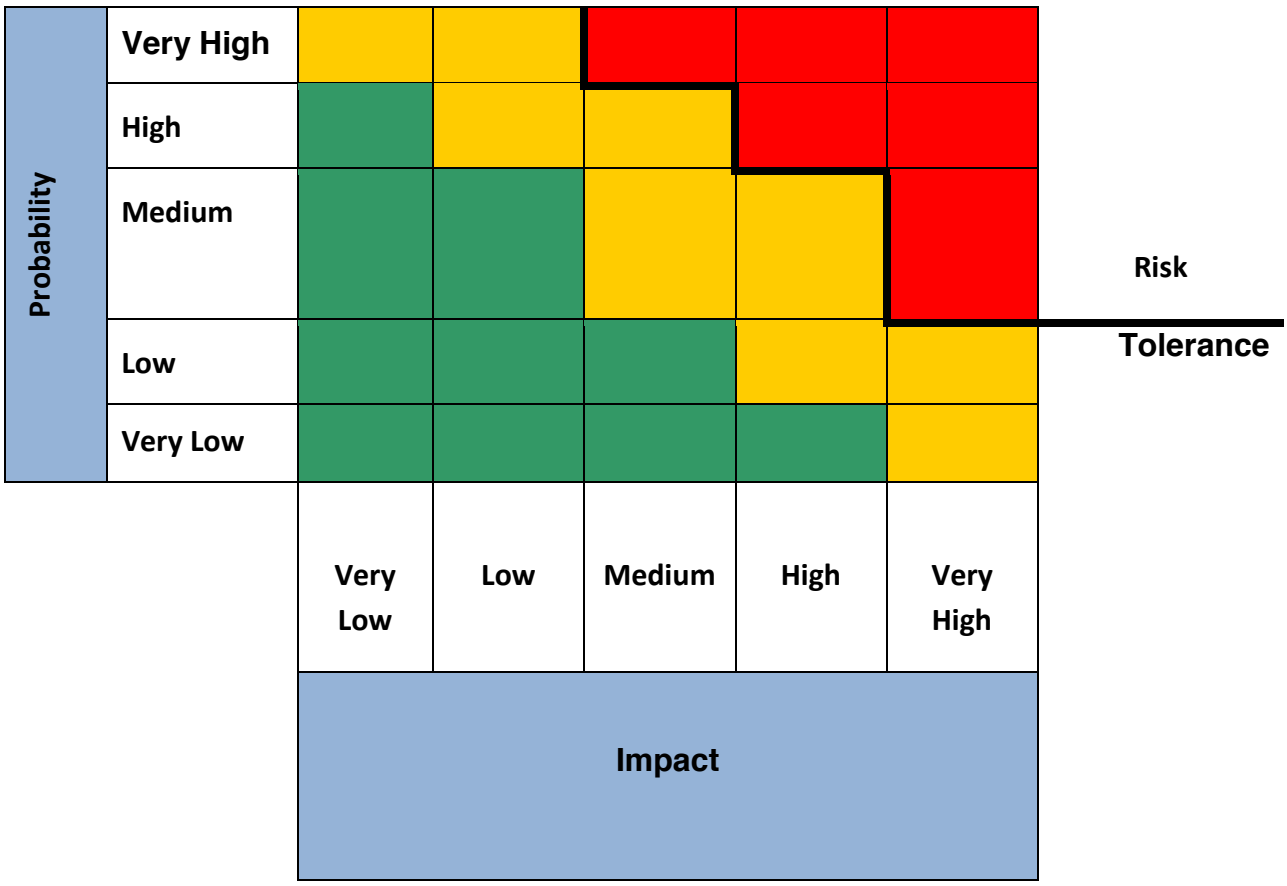


Table 3 – Proximity greater than 3 months



Example:

If today is 01/10/2012 and a risk is recorded with:

Probability = Medium

Impact = High

Proximity = 20/01/2013

The RAG Status will be set to **AMBER**.

If the values are not changed then after 21/01/2013 RAG Status will be set to **RED**.

Appendix 5 – MOR Definition of Risks and Responses

A5.1 Definitions

The following extracts from the **MANAGEMENT OF RISK GUIDANCE FOR PRACTITIONERS** manual give definitions of Threat, Risk and Issue and an explanation of the differences.

Item	Definition
Threat	A threat is a factor that could lead to a risk occurring, i.e. will be the cause of a risk. For example, there is a general shortage of skilled project managers. If that threat becomes reality in an organisation, there is a consequent risk that the project team may not have adequate skills and experience.
Risk	Risk is uncertainty of outcome (whether positive opportunity or negative threat). It is the combination of the chance of an event and its consequences.
Issue	An issue is a concern that cannot be avoided such as an unrealistic timescale for delivering a project, whereas a risk may not actually materialise. Once an issue is defined it can be managed through the appropriate Issue Process.

Entries in the Risk Register must be confined to actual risk and must be clearly stated in terms of the cause and effect. For example:

- 'The delivery of third party component XXXX may be delayed' is a threat not a risk. To define the risk the 'effect' information needs to be included, e.g. 'which will result in Project AAAA missing its Test Start date of dd/mm/yy and could delay the Launch Date'
- 'Technical specialist XXXX is unable to commit sufficient time to the project due to his system support commitments' is an issue not a risk. It should be reported and managed through the appropriate issue process
- 'Technical specialist XXXX may be unable to commit sufficient time to the project due to his system support commitments. This could result in delay in the delivery of component YYYY with consequent impact on other project delivery dates' is a risk because it is something that might happen and its possible effects have been stated

A5.2 Responses

Decisions will need to be made on how to respond to a specific risk by taking action to improve the situation. This action should result in a reduction in either or both of the likelihood and the impact of a risk. Example responses are shown in the table below.

Response	Explanation
Treating risk	Take action to control it by applying containment or contingent actions: • Containment actions are applied before a risk materialises. They are intended to lessen the likelihood of a risk or the consequences. • Contingent actions are those that are put into action after a risk has happened, but can be pre-planned so that people know what to do in advance. The focus is on reducing the impact of a risk.
Terminating risk	Doing things in a different way, where feasible, can entirely remove a risk.
Tolerating risk	It may be that nothing to reduce a risk can be done at reasonable cost. It such a case the risk should continue to be monitored to ensure it remains tolerable.
Transferring risk	It may be possible to transfer some or all aspects of a risk; perhaps by paying a third party to take on the venture that has the risk or by taking out insurance to lessen some of the impact of the risk.

Appendix 6 – Risk Management Methodology

The following Risk Management Methodology involves the identification, analysis and response to a programme/project risk. A risk can be any event that may have an adverse effect to a programme.

This 4-step risk methodology centres on a proactive approach to risk management where early detection, analysis and response lead to more effective results and reduced threat to a project or programme. This approach supports the goal of managing a risk versus reacting to one.

Step 1. Risk Identification - Identify and classify potential risks

A. Input:

- Event with a potentially adverse effect to a project or programme

B. Process and Tools:

- Determine source of input
- Determine whether risk is internal (within programme control) or external (out of programme control). **Note:** If external, consult with other programme/project stakeholders to determine accountability

C. Output:

- Identified risk
- Source of risk

Step 2. Risk Analysis - Qualify and quantify risk.

Input:

- Identified risk (from Step 1)
- Source of Risk (from Step 1)

B. Process and Tools:

- Qualify Risk (Determine the type of risk):

  - Business
  - Technology
  - Project
  - Operational Readiness
  - Resource

- Estimate Level of Impact (Determine impact against measurable variables):
  - Cost
  - Project Timeline
  - Resources
  - Project Deliverables
- Estimate Level of Probability (Estimate probability that a given risk event will occur):
  - Tool - Risk Probability Matrix
- Determine Stakeholder Risk Tolerance (Determine level of tolerance each stakeholder may have against a potential risk)
  - Interviewing stakeholders may provide both quantitative and qualitative information for measuring risk tolerance
- Identify Potential Risk Events (Determine potential discreet events that may arise as a result of the risk):
  - Tool - Decision trees
  - Tool - Process flow charts
- Obtain stakeholder input to verify Risk Analysis

C. Output:

- Complete Risk Analysis (Qualitative and Quantitative)

Step 3. Risk Response - Development of contingencies against each identified potential risk event

A. Input:

- Complete Risk Analysis (from Step 2)

B. Process and Tools

- Contingency Plans should be developed for each potential risk event. Plans should incorporate actions to address the following for each risk event where applicable:
    - **Terminating Risk (Risk Avoidance).** Outline steps to be taken to eliminate a potential risk. This can usually be accomplished by addressing the initial cause identified in Step 1.
    - **Treating Risk (Risk Mitigation).** Outline steps to be taken to reduce a potential risk.
    - **Tolerating Risk (Risk Acceptance).** Based on the risk analysis, certain risks may be neither avoidable nor reducible. In this event, alternative operational procedures should be outlined in light of the inevitable risk. Note: These risks are usually identified as external (in Step 1) such as economical, social and political events that impact a project.
    - **Transferring Risk (Risk Transfer).** Outline steps to be taken to transfer a Risk such as taking out insurance or paying a Third Party to manage the Risk.
- Provisioning (Obtain additional reserves to mitigate potential risk events):
    - Funding
    - Resources
    - Time
- Contractual Agreements (Contractual agreements may be entered into for insurance, services and other items as appropriate to avoid or mitigate risks):
    - Legal contracts, agreements, and other binding documents

C. Outputs:

- Contingency Plans
- Provisions

- Contractual Agreements

Step 4. Risk Response Implementation - This will vary based on the type of risk, its potential risk events and the associated contingencies developed for those events.

A. Inputs:

- Contingency Plans (from Step 3)
- Provisions (from Step 3)
- Contractual Agreements (from Step 3)

B. Processes and Tools:

- Implementation of the contingency plans, provisioning activities, and contractual agreements as needed to avoid or mitigate a risk event
- Ongoing monitoring of risk event with implemented contingency plan to ensure avoidance or mitigation.
- Documentation of risk management life cycle Serves as reference and “lessons learned” document for future risk management efforts.

C. Outputs:

- Corrective Action-Mitigation or avoidance of risk
- Risk Management Lifecycle Document.

Insync Supply Chain Management (see Comments or NOTES sheet for a description of the fields and their usage)

Strand / Programme	Project/Study Name	Project/Study Number	Project ID	Risk Number	Raised By	Date Raised	Risk Status	RAG Status	Probability	Impact	Proximity	Description of Risk	Impact Description	Trigger	Original Level	Current Level	Risk Owner	Possible Actions	Chosen Action	Action Owner	Action Status	Date of Last Update	Action Target Date	Issue Number	Closure Date	Mitigation Cost	% Like-lihood	Risk Budget
									VeryLow	VeryLow																		
									Low	Low																		
									Medium	Medium																		
									High	High																		
									VeryHigh	VeryHigh																		
									VeryHigh	VeryHigh																		
									VeryHigh	VeryHigh																		

Field	Description	Reference Documents / Notes
Strand / Programme	The owning Strand or Programme	
Project/Study Name	Name of the Project/Study at risk	
Project/Study Number	Reference Number for the Project/Study at risk .	
Project ID	The Project ID for the Project/Study at Risk .	
Risk Number	Unique identifier, allocated sequentially.	
Raised by	Name of individual who raised the risk.	
Date Raised	Date on which the risk was raised (format dd/mm/yy).	
Risk Status	The status of the register entry, one of: **OPEN** **CLOSED** **TRANSFER TO ISSUE**	
RAG Status	Current RAG status of the actual risk. Automatically determined from the **RAG MATRIX** using a combination of Probability, Impact and Proximity.	See **RAG MATRIX GRAPHIC** sheet for visual representation of table held in **RAG MATRIX** sheet.
Probability	The likelihood of the risk being realised, one of: **VERY LOW** **LOW** **MEDIUM** **HIGH** **VERY HIGH**	See **GUIDANCE** sheet for explanation of standard evaluation criteria .
Impact	The effect that the realisation of the risk would have, one of: **VERY LOW** **LOW** **MEDIUM** **HIGH** **VERY HIGH**	See **GUIDANCE** sheet for explanation of standard evaluation criteria .
Proximity	A date to indicate the potential timing of the risk (format dd/mm/yy or mmm-yy), i.e. whether the risk is immediate or likely to occur at some point in the future. If the risk is immediate then leave blank.	

Field	Description	Reference Documents / Notes
	If the risk will occur at some future point enter the future date. The date may change throughout the life of the risk as circumstances change. This date, along with Probability and Impact, will be used to determine the RAG Status.	See **GUIDANCE** sheet for more explanation.
Description of Risk	This must be clearly stated in terms of cause and effect along the lines of '**There is a risk of/that……..which may result in……..**'	see **Risk Management Process - Definition of Risk and Responses**
Impact Description	A more comprehensive description of Impact if this is required.	
Trigger	Used in conjunction with Proximity. If the risk will only manifest itself, or will grow stronger, due to some future event or circumstance then details should be recorded.	See **GUIDANCE** sheet for more explanation.
Original Level	The initial management level for the risk, one of: **IM BOARD** (= Information Management Board level) **SUB COMMITTEE** (= Strand/Programme Sub Committee Level) **PROJECT** (= Project Manager or within project)	See **Risk Management Process - Guidance on Setting Risk Level & Escalation**
Current Level	The current management level for the risk. At creation, this should be set to the same value as Original Level. Over time it will indicate escalation or demotion of a risk when compared with Original Level.	See **Risk Management Process - Guidance on Setting Risk Level & Escalation**
Risk Owner	Name of individual responsible for managing the risk.	
Possible Actions	A list of possible actions that could be taken in response to the risk.	
Chosen Action	The selected action(s) to be taken. This field must be completed at Creation even if the only known action at that time is to further analyse the risk to determine possible responses.	
Action Owner	Name(s) of individual(s) responsible for implementing action(s).	
Action Status	A succinct description of the current progress towards completion of action(s).	
Date of Last Update	Date on which the risk entry was last updated.	

Field	Description	Reference Documents / Notes
Action Target Date	Target date for completion of Chosen Action (format dd/mm/yy).	
Issue Number	To maintain an audit trail to the Issue Register. If the risk originated as an Issue then record the original Issue Number. If the risk is transferred to the Issue Register then record the resulting Issue Number.	
Closure Date	The date on which the risk is **CLOSED** or **TRANSFER TO ISSUE** (format dd/mm/yy).	
Mitigation Cost	Can be used to record the cost of mitigation action.	
% Likelihood	Used in conjunction with Mitigation Cost. This is the Probability of the risk expressed as a % for budgeting purposes.	
Risk Budget	To hold the result of Mitigation Cost X % Likelihood to give a provision for treating the risk. If a calculation is done for all known risks on a project then the total provides a budget provision for the treatment of risk for the whole of the project.	

Guidance on Setting Probability, Impact and Proximity

Probability

Use the Criteria in the table below to assess the likelihood of a risk being realised and assign the Probability shown for that level. The three types of Criteria shown are just different ways of expressing the same level of likelihood.

Probability	Criteria		
Very Low	Virtually impossible	< 5% likelihood	Odds > 20/1
Low	Low but not impossible	5% to 20% likelihood	Odds 20/1 to 5/1
Medium	Fairly likely	21% to 50% likelihood	Odds 5/1 to 2/1
High	More likely than not	51% to 80% likelihood	Odds 2/1 to 4/5
Very High	Virtually certain	> 80% likelihood	Odds < 4/5

Impact

Impact on an activity is usually considered in terms of the effect on cost, scheduling and quality. Each of these will need to be understood in terms of its importance to the activity. Once relative importance is understood, use the Criteria in the table below to assess the effect of a risk being realised and assign the Impact shown for that level.

Impact	Budget Criteria	Schedule Criteria	Quality Criteria
Very Low	Negligible effect on cost, < 3%	Negligible effect on schedule, < 3%	System will fully meet mandatory requirements.
Low	Small increase in cost, 3 to 10%	Small schedule slip, 3 to 10%	A few shortfalls in desirable functionality
Medium	Significant increase in cost, 10 to 30%	Significant schedule slip, 10 to 30%	Minor shortfalls in one or more key requirements
High	Large increase in cost, 30 to 75%	Large slip in schedule, 30 to 50%	Major shortfall in one or more key requirements
Very High	Major increase in cost, > 75%	Major slip in schedule, > 50%	Major shortfall in any of the critical requirements

Proximity

Proximity reflects the timing of the risk.

If the risk is immediate then there is no need to specify Proximity. However, if a risk will only arise at some future date or as a result of some future event then a future date will be recorded.

For instance, if a parallel development or operational upgrade is intending to implement changes prior to the end of your project then there may be a risk that the changes will impact your project. However, the changes may not be implemented or may be implemented only in areas that don't affect your project or may be piloted then rolled out when all risks are eliminated. Any potential risk to your project will only arise as the changes are implemented so the Proximity should be given the date of the intended implementation and the risk should be re-evaluated in the light of new knowledge gained as the date approaches.

Trigger

A further optional field is included in the Risk Register to be used in conjunction with Proximity. It allows for the recording of a description of any future event that generated the Proximity date and for any notes or comments that may be required.

Field	Description
Strand / Programme	The owning Strand or Programme
Project/Study Name	Name of the Project/Study at risk
Project/Study Number	Reference Number for the Project/Study at risk .
Project ID	The Project ID for the Project/Study at Risk .
Risk Number	Unique identifier, allocated sequentially.
Raised by	Name of individual who raised the risk.
Date Raised	Date on which the risk was raised (format dd/mm/yy).
Risk Status	The status of the register entry, one of: **OPEN** **CLOSED** **TRANSFER TO ISSUE**
RAG Status	Current RAG status of the actual risk. Automatically determined from the **RAG MATRIX** using a combination of Probability, Impact and Proximity.
Probability	The likelihood of the risk being realised, one of: **VERY LOW** **LOW** **MEDIUM** **HIGH** **VERY HIGH**
Impact	The effect that the realisation of the risk would have, one of: **VERY LOW** **LOW** **MEDIUM** **HIGH** **VERY HIGH**
Proximity	A date to indicate the potential timing of the risk (format dd/mm/yy or mmm-yy), i.e. whether the risk is immediate or likely to occur at some point in the future. If the risk is immediate then leave blank.

Field	Description
	If the risk will occur at some future point enter the future date. The date may change throughout the life of the risk as circumstances change. This date, along with Probability and Impact, will be used to determine the RAG Status.
Description of Risk	This must be clearly stated in terms of cause and effect along the lines of '**There is a risk of/that……..which may result in……**'
Impact Description	A more comprehensive description of Impact if this is required.
Trigger	Used in conjunction with Proximity. If the risk will only manifest itself, or will grow stronger, due to some future event or circumstance then details should be recorded.
Original Level	The initial management level for the risk, one of: **IM BOARD** (= Information Management Board level) **SUB COMMITTEE** (= Strand/Programme Sub Committee Level) **PROJECT** (= Project Manager or within project)
Current Level	The current management level for the risk. At creation, this should be set to the same value as Original Level. Over time it will indicate escalation or demotion of a risk when compared with Original Level.
Risk Owner	Name of individual responsible for managing the risk.
Possible Actions	A list of possible actions that could be taken in response to the risk.
Chosen Action	The selected action(s) to be taken. This field must be completed at Creation even if the only known action at that time is to further analyse the risk to determine possible responses.
Action Owner	Name(s) of individual(s) responsible for implementing action(s).
Action Status	A succinct description of the current progress towards completion of action(s).
Date of Last Update	Date on which the risk entry was last updated.
Action Target Date	Target date for completion of Chosen Action (format dd/mm/yy).

Field	Description
Issue Number	To maintain an audit trail to the Issue Register. If the risk originated as an Issue then record the original Issue Number. If the risk is transferred to the Issue Register then record the resulting Issue Number.
Closure Date	The date on which the risk is **CLOSED** or **TRANSFER TO ISSUE** (format dd/mm/yy).
Mitigation Cost	Can be used to record the cost of mitigation action.
% Likelihood	Used in conjunction with Mitigation Cost. This is the Probability of the risk expressed as a % for budgeting purposes.
Risk Budget	To hold the result of Mitigation Cost X % Likelihood to give a provision for treating the risk. If a calculation is done for all known risks on a project then the total provides a budget provision for the treatment of risk for the whole of the project.

Reference Documents / Notes
See **RAG MATRIX GRAPHIC** sheet for visual representation of table held in **RAG MATRIX** sheet.
See **GUIDANCE** sheet for explanation of standard evaluation criteria .
See **GUIDANCE** sheet for explanation of standard evaluation criteria .

Reference Documents / Notes
See **GUIDANCE** sheet for more explanation.
see **Risk Management Process - Definition of Risk and Responses**
See **GUIDANCE** sheet for more explanation.
See **Risk Management Process - Guidance on Setting Risk Level & Escalation**
See **Risk Management Process - Guidance on Setting Risk Level & Escalation**

Insync Supply Chain Management

Reference Documents / Notes

		DEFAULT RAG (Used on ALL projects)		
PROBABILITY	IMPACT	PROXIMITY		
		< 1 month	1 to 3 months	> 3 months
Very Low	Very Low	GREEN	GREEN	GREEN
Very Low	Low	GREEN	GREEN	GREEN
Very Low	Medium	AMBER	GREEN	GREEN
Very Low	High	AMBER	AMBER	GREEN
Very Low	Very High	RED	AMBER	AMBER
Low	Very Low	GREEN	GREEN	GREEN
Low	Low	AMBER	GREEN	GREEN
Low	Medium	AMBER	AMBER	GREEN
Low	High	RED	AMBER	AMBER
Low	Very High	RED	RED	AMBER
Medium	Very Low	AMBER	GREEN	GREEN
Medium	Low	AMBER	AMBER	GREEN
Medium	Medium	RED	AMBER	AMBER
Medium	High	RED	RED	AMBER
Medium	Very High	RED	RED	RED
High	Very Low	AMBER	AMBER	GREEN
High	Low	RED	AMBER	AMBER
High	Medium	RED	RED	AMBER
High	High	RED	RED	RED
High	Very High	RED	RED	RED
Very High	Very Low	RED	AMBER	AMBER
Very High	Low	RED	RED	AMBER
Very High	Medium	RED	RED	RED
Very High	High	RED	RED	RED
Very High	Very High	RED	RED	RED

HighHigh<1	RED
HighHigh>3	RED
HighHigh1-3	RED
HighLow<1	RED
HighLow>3	AMBER
HighLow1-3	AMBER
HighMedium<1	RED
HighMedium>3	AMBER
HighMedium1-3	RED
HighVeryHigh<1	RED
HighVeryHigh>3	RED
HighVeryHigh1-3	RED
HighVeryLow<1	AMBER
HighVeryLow>3	GREEN
HighVeryLow1-3	AMBER
LowHigh<1	RED
LowHigh>3	AMBER
LowHigh1-3	AMBER
LowLow<1	AMBER
LowLow>3	GREEN
LowLow1-3	GREEN
LowMedium<1	AMBER
LowMedium>3	GREEN
LowMedium1-3	AMBER
LowVeryHigh<1	RED
LowVeryHigh>3	AMBER
LowVeryHigh1-3	RED
LowVeryLow<1	GREEN
LowVeryLow>3	GREEN
LowVeryLow1-3	GREEN
MediumHigh<1	RED
MediumHigh>3	AMBER
MediumHigh1-3	RED
MediumLow<1	AMBER
MediumLow>3	GREEN
MediumLow1-3	AMBER
MediumMedium<1	RED
MediumMedium>3	AMBER
MediumMedium1-3	AMBER
MediumVeryHigh<1	RED
MediumVeryHigh>3	RED
MediumVeryHigh1-3	RED
MediumVeryLow<1	AMBER
MediumVeryLow>3	GREEN
MediumVeryLow1-3	GREEN
VeryHighHigh<1	RED
VeryHighHigh>3	RED
VeryHighHigh1-3	RED
VeryHighLow<1	RED
VeryHighLow>3	AMBER
VeryHighLow1-3	RED
VeryHighMedium<1	RED
VeryHighMedium>3	RED
VeryHighMedium1-3	RED
VeryHighVeryHigh<1	RED
VeryHighVeryHigh>3	RED
VeryHighVeryHigh1-3	RED
VeryHighVeryLow<1	RED
VeryHighVeryLow>3	AMBER
VeryHighVeryLow1-3	AMBER
VeryLowHigh<1	AMBER
VeryLowHigh>3	GREEN
VeryLowHigh1-3	AMBER

Insync Supply Chain Management

VeryLowLow<1	GREEN
VeryLowLow>3	GREEN
VeryLowLow1-3	GREEN
VeryLowMedium<1	AMBER
VeryLowMedium>3	GREEN
VeryLowMedium1-3	GREEN
VeryLowVeryHigh<1	RED
VeryLowVeryHigh>3	AMBER
VeryLowVeryHigh1-3	AMBER
VeryLowVeryLow<1	GREEN
VeryLowVeryLow>3	GREEN
VeryLowVeryLow1-3	GREEN