

HRA Risk Management Procedure

**Author:** Stephen Tebbutt

**Date of Release:**

**Version No. & Status:** 2.4, 12.01.2015, FINAL

**Approved By:**

**Supersedes Version:**  2.3, 03.12.2014

**Review Date:** 1 year after approval

**Owner:** Janet Wisely

# Purpose

* 1. The purpose of this document is to set out how the HRA carries out its risk management and corporate assurance policy. Specifically it will:
     1. Describes risk management roles and lines of responsibilities
     2. Describe the risk management process to:
        1. Provide guidance to Directorate Risk Managers on how the HRA identifies and manages its strategic, operational, programme and project risks at directorate and organisational level;
        2. Describe how risks to the HRA are to be evaluated thereby facilitating consistency in the evaluation and classification of risk across the organisation;
        3. Describe the criteria for escalation of risks from a Directorate risk register to the Corporate risk register
        4. Provide guidance on managing cross-division related risks, both internally and with external stakeholders;
        5. Identify frequency of reporting risks to corporate level.
     3. Provide guidance regarding how risk registers should be completed;

# Scope

* 1. The HRA recognises that risk management is an integral part of the management and working processes of the organisation. Risk management is part of the culture of the HRA and will be continually evaluated.
  2. The HRA will communicate the message that all staff have a role to play in managing risk throughout the whole organisation, and provide the means for them to play that role through the dissemination of relevant information and training.
  3. The HRA, when working with other partners in the NHS and in the wider health environment, will seek to develop collaborative risk management arrangements, recognising that integrating risk with partner organisations can be complex. The HRA will endeavour to ensure that ownership of the risk is confirmed at the outset with a forum agreed for the communication and management of the risk.

# Reference Documents

* 1. This procedure should be read in conjunction with the HRA Risk Management and Corporate Assurance Policy document which sets out the HRA’s risk management principles and system used to underpin the risk management strategy for the organisation.

# Responsibilities

## HRA Board

* + 1. The Board has overall responsibility for risk management throughout the HRA. Specific activities they are responsible for include:
       1. Agreeing and reviewing the Risk Management Policy. The Board should review the policy on a yearly basis to ensure it is relevant and supportive of the HRA’s current strategy and activities;
       2. Assigning a Responsible Senior Manager with oversight of Risk Management and who is responsible for championing risk management at HRA;
       3. Ensuring risk management is embedded into all processes. The Board needs to assure themselves that risk management is being undertaken and risk controls and contingencies are in place and verified as an integral part of the HRA’s working processes. This assurance is ultimately provided through the Governance Statement within the HRA’s Annual Report and Accounts and based on the work of the Audit and Risk Committee;
       4. Reviewing the risks identified in the Corporate risk register on a quarterly basis. The Board needs to assure themselves that the HRA has appropriately identified the risks associated with its strategy, and has put in place appropriate risk management controls and contingency plans and that they accept the residual risk.
       5. Ensure that the appropriate structure exists within the HRA to ensure risk management processes are effective at dealing with risks, controls, contingencies and action plans, including defined Audit and Risk Committee and people responsibilities.
  1. **Audit and Risk Committee**
     1. The Audit and Risk Committee is the sub-committee of the Board that provides assurance and has the responsibility for overview of the audit arrangements of the HRA in order to ensure its main activities demonstrate effective control, good governance and risk management with regard to the achievement of objectives and obligations of the organisation. Specific activities are:
        1. Reviewing the Corporate risk register after submission to EMT;
        2. Commissioning Internal Audit Reports on risk management as required;
        3. Reviewing the draft Governance Statement based on the opinions received from Internal and External Audit and assurance that the HRA’s risk management responsibilities and objectives are being met.
        4. Ensures that all HRA staff and other relevant stakeholders including the general public are made aware of relevant risk issues and any action which it wishes them to take. This process also forms part of the risk identification process by affording the opportunity for those not directly involved in risk management to make a contribution, and in doing so, complete the cycle of risk management.
  2. **Internal Audit and External Audit**
     1. The Internal Audit function provided by the Department of Health will form part of the review process and will provide opinions on the risk management process carried out within the HRA and the validity of any Board declarations on this subject. The Internal Auditors will advise the Audit and Risk Committee accordingly. They will:
        1. Audit the risk management activities and systems for the HRA from the corporate / strategic level down to the organisational / project level. They will take a risk based approach to their audits, such that the organisation’s objectives which potentially contain the greatest risk to organisational success are focused on;
        2. Their audit will include assurance / verification of both the risk management system activities and critical risk management controls and contingencies;
        3. They will provide an audit report which will include findings to aid the HRA improve and develop its risk management activities in such a way as to support the organisation’s business.
        4. Provide advice throughout the year to HRA staff as needed;
        5. Impartially evaluates HRA’s risk management system and the Corporate risk register.
        6. Reports to the Audit and Risk Committee.
  3. **Executive Management Team (EMT)**
     1. The HRA’s EMT is the group which undertakes the high level risk assessment by reviewing all risks scored as 12 and over and oversees the directorate level risk management activities and progress. As such, EMT will:
        1. Undertake the organisation’s high level risk assessment as part of the annual business planning activities, and will update the assessment on a quarterly basis based on developments throughout the year;
        2. Ensure that risk controls and contingencies are implemented. This can be achieved as part of the quarterly business reviews of progress against annual targets;
        3. Review the Corporate risk register quarterly with regard to the status of risks at a corporate and operational level and the progress of control implementation, contingencies and actions plans.
     2. EMT members will be responsible for overseeing risks and the controls, contingencies and actions in place or developed to ensure these risk levels are acceptable to the organisation. EMT members will also be responsible for managing their own specific directorate risks through Directorate Risk Registers.
     3. EMT is responsible for ensuring staff are aware of their role in managing risk with appropriate guidance and training provided as required.
  4. **Responsible Senior Manager for Risk**
     1. The Responsible senior manager is responsible for ensuring that the risk management requirements of the Board are implemented in accordance with their requirements
     2. Currently responsibilities are as follows:
        1. Ensuring all required risk management systems, policy and strategy and support are in place (Chief Executive, Director of Finance, Board secretary)
        2. Scheduling and facilitating Internal Audit activities; (Director of Finance)
        3. Regularly reviewing and following-up risk management activities with all parties. This will include ensuring the verification / assurance of risk management activities and key controls/contingencies; (Board secretary)
        4. Writing the Governance Statement; (Chief Executive, Director of Finance, Board Secretary)
        5. Ensuring the appropriate risk structure is in place including the Audit and Risk Committee; (Board Secretary)
        6. Monitoring risk performance. As part of the routine progress reports the Audit and Risk Committee receives information on the risk performance in terms of the current risk profile, risk management activity performance, and implementation and verification of risk management controls and contingencies. (Board secretary)
  5. **Board Secretary**
     1. The post holder is responsible for coordinating the combined Corporate and Directorate risk registers. This includes the Corporate risk register, Corporate part 2 confidential risk register and individual directorate risk registers.
     2. The post holder is responsible for ensuring all risks with a score of 12 and over are reviewed by EMT on a quarterly basis and compiling the corporate risk register of those risks EMT has identified as requiring escalation to the Board.
     3. The post holder will be responsible for ensuring all risk register owners are aware when the EMT review periods are throughout the year and provide them with sufficient time to update their register.

* 1. **Directorate Risk Manager**
     1. Directorates lead most of the activities of the HRA and as such they also manage the risks at the programme, day to day operational and project levels. Directorate Risk Managers are responsible for the overall coordination, monitoring and management of their individual Risk Register.
     2. Directors may delegate the coordination of the risk register to a senior individual within their team however the director is ultimately responsible for their risks (they will always be the risk owner) and compiling their risk register; t. The delegated individual should be experienced enough to take ownership of the division’s risk management agenda and in a position to drive the division risk management activities, including being able to implement corrective actions if needed;
     3. The Director, or delegated individual, will be responsible for liaising with each Action Owner (person who is managing a particular risk) and cross division risk managers for cross division risks, and ensuring that Risk Owners are aware of the risks they are responsible for.
     4. Risks will be identified and assessed, with appropriate controls and contingencies developed. This will be done:
        1. In accordance with the annual planning process for the programme risks, with reviews and updates as needed throughout the year.
        2. In accordance with the project planning and management process for all projects. Note: The different nature of projects in the HRA means that the risk assessment and management approaches will vary between projects according to their size, complexity and potential risk to the organisation.
        3. For day to day operational activities on a regular basis or when changes in processes are being implemented. Note: The different nature of operational activities in the HRA means that the risk assessment approaches will vary according to their size, complexity and potential risk to the organisation and of the activity being assessed.
        4. Monitor and maintain their own risk registers on an ongoing basis. The quarterly progress against the business plan should include the division’s assessment of their risks, and risk management controls, contingencies and actions.
  2. **Programme Management Office**
     1. The Programme Management Office (PMO) will be responsible for ensuring any risks related to PMO coordinated projects are managed appropriately. This will involve the completion and regular review of individual project risk registers. The risk registers will follow the same format as the directorate risk registers.
     2. The PMO will ensure that project managers are made aware of their responsibility to:
        1. identify risks related to their project
        2. identify and manage the actions necessary to mitigate project-related risks
        3. regularly review (usually monthly) risks as part of their project governance
        4. provide the PMO with recommended updates to existing risk and information on new risks
     3. The PMO will:
        1. Collate the recommended updates for approval by the relevant Director on a regular basis
        2. Once approved by the relevant Director, input these changes into the risk register
        3. Provide monthly risk register reports (filtered by the relevant project) to the project manager and/or project board for review
  3. **Person/Group Raising Risk**
     1. Source of risk which could come from a Project Team, management group, programme boards or an individual person within a directorate.

* 1. **Risk Owner**
     1. Person who is accountable for a particular risk. This will always be a Director, though they can delegate responsibility for managing the risk to the Action Owner.
  2. **Action Owner**
     1. Person responsible for monitoring and mitigating a particular risk in the Directorate Risk Register.
  3. **External Stakeholder Involvement**
     1. External stakeholders such as government or regulatory bodies, research bodies, reference groups, the public and patients are encouraged to be part of the risk identification process where applicable especially at the planning stages of a project.

1. **Risk Management Process**
   1. The following flow chart describes the risk management process:

## Identify the risk

* + 1. The first step is to identify the risk. There is no unique method for identifying risks and risks may be identified from a number of sources in a variety of ways including, but not limited to, the following:
       1. Risk assessment of everyday operational activities, especially when there is a change in working practice or environment
       2. Horizon scanning
       3. Performance management of key performance indicators
       4. Internal audit reviews and assurances
       5. Annual planning cycle
       6. Complaints, incidents, claims and general observations
       7. Staff consultation and surveys
       8. National recommendations
       9. Information from key stakeholders

## There are two distinct phases to risk identification:

## Initial Risk identification - relevant to new services, new techniques, projects

## Continuous Risk Identification – relevant to existing services and should include new risks or changes in existing risks e.g. external changes such as new guidance, legislation etc.

* + 1. In some cases risks may already have been identified and logged on a risk register, so checks will need to be made by the Risk Manager to avoid duplication.

## Investigate the risk

## Once the risk has been identified it needs to be investigated and raised to the relevant risk register. A Risk Owner needs to be assigned.

* + 1. Project and non-project Related Risks
       - 1. Initially it needs to be decided if the risk is project or non-project related (e.g. operational). A separate risk register will be held for each project the PMO is responsible for and updated by a member of the project team or PMO. These will be added to the corporate risk register on a quarterly basis.
         2. Occasionally, for substantial and reputationally important projects or programmes e.g. HRA Approval, an individual tab on the corporate risk register will be created and managed by the PMO and relevant Director.
         3. Any non-project risks (e.g. operational) identified should be raised and managed by the relevant Director or assigned individual and added to the relevant directorate risk register.
    2. Risks identified from an incident
       1. A risk may also be identified from the occurrence of an incident. If an risk arises because a health and safety or business incident has occurred, then it should be reported following the relevant procedure guidelines.
       2. Employees should refer to:
          1. HRA Information risk policy and security incident report form: <https://intranet.hra.nhs.uk/system/files/HRA%20Information%20Risk%20Policy%20and%20Security%20Incident%20Report%20Form%20Final%20V%201.2%20April%202014%20Board%20Approved.pdf>
          2. HRA Health and Safety Incident Reporting Policy: <https://intranet.hra.nhs.uk/system/files/HRA%20Health%20and%20Safety%20Incident%20Reporting%20Policy%20v%201.0%20Final%20July%202013.pdf>
          3. Whistleblowing policy and procedure: <https://intranet.hra.nhs.uk/system/files/HRA%20Whistleblowing%20Policy%20and%20Procedure%20V1.0%20Final_2.pdf>
    3. Cross cutting or shared risks
       1. The HRA recognises that some of its risks will be shared between different directorates within the organisation and also across external stakeholders.
       2. For internal directorate shared risks, the HRA will seek to ensure that a clear decision is made regarding which Director is ultimately responsible for the overall management and coordination of the risk.
       3. For risks which involve external stakeholders, the HRA will ensure that a decision is taken regarding who will assume the overall responsibility for the risk and the communication mechanism for the management of the risk. The HRA would normally look for the risk to be managed by the originating organisation or the organisation which has the primary mandate for the management of the activity.
       4. In both instances the HRA will ensure that ownership of the risk is confirmed at the outset with a forum agreed for the communication and management of the risk. This will be captured in the risk register and any relevant risk actions from the forum recorded.

* + 1. Identify when the risk was raised
       1. The date of when the risk is initially raised should be inserted in the ‘Date Raised’ column.
    2. Identify who should own and manage this risk
       1. Every risk raised should have a Risk Owner (person accountable for the risk should it occur) and an Action Owner (person managing the risk).
       2. In the event that a risk is raised by one director but the appropriate owner/lead is within another division, both Directors should liaise with each other to confirm the Risk Owner and Lead.
  1. **Evaluate the Risk**
     1. The likelihood and impact of the risk should be assessed using a Risk Matrix before the score is entered onto the risk register.
     2. All risks will be evaluated using the following 5x5 matrix.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **IMPACT** | **Very high  5** | **5** | **10** | **15** | **20** | **25** |
| **High 4** | **4** | **8** | **12** | **16** | **20** |
| **Medium 3** | **3** | **6** | **9** | **12** | **15** |
| **Low 2** | **2** | **4** | **6** | **8** | **10** |
| **Very low 1** | **1** | **2** | **3** | **4** | **5** |
|  |  | **1 Rare** | **2 Unlikely** | **3 Possible** | **4 Likely** | **5 Almost certain** |
|  |  | **LIKELIHOOD** | | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Likelihood** | **Impact** | **Consequence (Severity / Impact)** | |
| Impact on Strategic Objectives (Business Delivery) | Impact on Organisation |
| **5**  **ALMOST CERTAIN** | **5**  **CATASTROPHIC** | Will result in failure to deliver SO | Major loss of credibility / reputation  Need to inform ministers / sponsors |
| **4**  **LIKELY** | **4**  **MAJOR** | Will have significant impact on the successful delivery of the SO | Significant impact on credibility / reputation  Need to inform EMT / Board |
| **3**  **POSSIBLE** | **3**  **MODERATE** | Will have some impact on the successful delivery of SO | Some impact on credibility / reputation  Manageable at EMT / Directorate level |
| **2**  **UNLIKELY** | **2**  **MINOR** | Possibility of minor impact on the successful delivery of SO | Minor impact on credibility / reputation  Manageable by senior managers / teams |
| **1**  **RARE** | **1**  **INSIGNIFICANT** | Will not impact on the successful delivery of SO | No impact on credibility / reputation |

* + 1. It is recognised that the assessment of risks against the “Consequence” criteria could result in varying interpretations and therefore it will be reviewed on a quarterly basis by EMT to assess the consistency of interpretation and also the context and requirement for potential escalation of the risk.

## Manage the risk

## Once the risk has been evaluated, it is time to identify the approach to managing the risk and develop an Action Plan. A risk can be managed in the following ways:

## Mitigation Reduce the likelihood of the risk occurring or limiting impact of risk

## Transference Move the ownership and management of the risk to another department or to a third party e.g. Insurance Company

## Termination Prevent the risk occurring by implementing different measures that eliminates the risk altogether

## Tolerance Accept the risk could occur as there are no measures feasible to reduce the likelihood or impact

## Contingency Identify mechanisms that can be implemented if the risk was to occur

* + 1. Escalate the risk to a higher level if necessary
       1. Directorate level risk should be escalated to EMT via the Board Secretary where the risk score is assessed at ≥ 12, or where the risk impact would have wider or organisational significance.
       2. Risks with a score of 20 and over should be escalated to the DH sponsor team.
  1. **Monitor and Review the Risk**
     1. Each directorate should review its risks, and the measures to control the risks, on a regular basis. This will feed into the quarterly reporting cycle of the Corporate risk register to the Board and DH sponsorship team.
     2. Reviews should ask the following questions:
        1. Are the risks identified still valid?
        2. Have there been any changes which have produced new risks?

* + - 1. Has the Action plan from risk assessments and past risk reviews been implemented?
      2. Are risk mitigations still adequate?
      3. Does the assurance show that the risk controls are in place and active?

1. **Action to Take if Risk Occurs**
   1. In the event a risk occurs, it should be recorded in the Issues Log. Any contingency plans identified should be implemented and the event reported to the Risk Owner for further action.
   2. The Director responsible for the risk register should be kept informed and EMT / Board notified depending on the severity and consequence of the risk.

# Completion of risk registers

# A risk register is used as a database to capture and manage risks at corporate, directorate and project level. The HRA uses Excel to hold this information. The Combined Corporate and Directorate risk register contains all risks for the organisation. Each directorate will use its own risk register as a management tool to capture all risks and score them according to the impact on their directorate at an operational and/or project level.

# All risk registers follow the same standard template which contains a number of mandatory columns. The risk registers are structured similarly to allow the efficient escalation of risks to other risk registers.

# The PMO will have access to the relevant risk registers which involve projects coordinated by the PMO. The PMO will collate any recommended updates, following the review of the risks by the relevant Board, for approval by the appropriate Director. Once approved by the Director these will be added into the risk register by the PMO.

# Whenever a change occurs to a risk register, the updated text should be formatted in red. When the risk register is brought to the appropriate Board or management group for review and approval it will facilitate the ease of identifying what, if anything, has changed since the last meeting. After the Board or group has reviewed the updated risk register, the text should be converted to black.

# Risk registers are password protected and only the relevant Director, or the individual assigned to manage the risk register, plus the Board Secretary and Corporate Secretary, and the PMO have access to the document. The register should be saved and protected after each use. The Board Secretary maintains a record of the passwords which is shared with the Corporate Secretary for business continuity purposes.

* 1. Appendix A describes the columns in the standard HRA risk register template with a description of what should be added. The risk register owner should ensure this is followed when completing the risk register.
  2. It is important to note that:
     1. Only one person may access the risk register, and make changes to the document, at any one time to avoid the loss of data. To ensure this takes place, an email, tagged under high importance, should be sent to colleagues with access to the risk register stating: *‘I am about to edit the risk register’*. Upon completion, a follow up email should be sent to the group stating *‘Editing of risk register complete’*.
     2. A file note detailing those with access to the risk register and whom the emails should be sent to is saved in the risk register folder. The Board Secretary is responsible for ensuring this document is kept up to date to ensure the relevant personnel are copied in.
     3. Any additional risks to be added, or current risks to be updated or closed, should be inputted directly into the document. No cut and pasting of data should take place to avoid the potential for the corruption to the file.
     4. When a new risk is allocated, it should be assigned the next available HRA risk register reference under the *‘master index’* tab by the person entering the risk onto the risk register. The directorate risk register reference should be added in the relevant column to show that the HRA risk reference has been taken.
     5. Terms, scales and symbols described on the *‘Risk Register explanatory note’* tab should only be used. The autofill colour coding in the *‘Timescale / Likelihood / Impact / Status and Target Residual’* columns should similarly not be altered as these are standardised across all Registers.
  3. When making changes to the document, the version tab at the top of the document should updated to show when the document was last modified. The last reviewed column should similarly be updated to reflect the date when the changes were made.
  4. If a risk has increased, decreased or remained the same, the ‘*status change since last report’* symbol should be updated accordingly.
  5. Any risks which have been deemed to be closed should not be deleted from the risk register. Risks should be marked as *‘Closed’* in the ‘*status change since last report’* columnand the row greyed out.

1. **Reporting Risks to the Corporate Level**
   1. All risks with a score of 12 and over will be escalated to EMT on a quarterly basis via the Board Secretary.
   2. EMT will review each risk in turn and consider whether it is a significant risk which should be reported to the Board and DH sponsor team.
   3. The Board Secretary will populate the Corporate risk register from those risks which EMT has agreed should be escalated further.
   4. Any risks which are confidential but require escalation to the Board or Sponsor will be incorporated into a Part 2 Corporate risk register by the Board Secretary.

* 1. All risks 20 and over will be escalated to the Department of Health Sponsor team.
  2. The EMT, Board (via the Audit and Risk Committee), Internal and External Audits may give feedback or request certain actions for specific risks e.g. re-score risk, change or add more key controls or require specific actions to be undertaken to address the risk. These requests will be communicated to the relevant Directorate Risk Manager via the Board Secretary for actioning.

1. Monitoring of activities covered by the procedure
   1. The activities covered in this procedure will be monitored on a regular basis by EMT, the responsible senor manager for risk and the Board Secretary.

# How lessons are learnt and incorporated into the procedure

* 1. The policy will be regularly reviewed with any lessons learnt from those using the procedure incorporated into future versions. Any lessons learnt should be sent to the HRA Board Secretary and Chief Executive Business Manager for recording and implementation.

# Management of Documents and Records

* 1. This Risk Management Procedure along with the Risk Management and Corporate Assurance Policy will be available on the staff intranet.
  2. The combined corporate and directorate risk registers are held on the shared drive at: [G:\Shared Drive\HRA Management\Risk Registers\NEW – 2014](file:///G:\Shared%20Drive\HRA%20Management\Risk%20Registers\NEW%20–%202014).
  3. The corporate and directorate risk register will be a moving and dynamic document which will be updated on an ad hoc basis. A snapshot of the risk register will be taken and archived on a monthly basis by the Board Secretary.
  4. This procedure will be reviewed on an annual basis by the Executive Management Group, and will require approval from the Board.

# APPENDIX A – Risk Register Column Headings

| **Column Heading** | **Description** | **Format** |
| --- | --- | --- |
| HRA risk reference | To uniquely identify a risk that has been raised onto any risk register | HRA000 |
| Dept. risk reference | To uniquely identify a risk on a directorate risk register | Dept/Project (initials) 000 |
| Risk type | Indicates type of risk for example, IT, reputational, financial, informatics etc. If a risk relates to a project, the name of the project should be detailed. | Free text |
| Date raised | Indicates when risk was first entered onto risk register | dd/mm/yyyy |
| Last reviewed | Indicates the last review date | dd/mm/yyyy |
| Risk description | Describes the risk, cause and effect | Free text.  (New line (alt + enter) for each description) |
| Timing | Describes timing as imminent – impact within 3 months, medium – impact within 6 months or longer term – impact over 6 months | Imminent / Medium / Long Term  (Colour automatically assigned by word) |
| Likelihood | Indicates score of probability of risk occurring from scale of 1 (low) to 5 (high) | Scale of 1 to 5  (Colour automatically assigned by number) |
| Impact | Indicates score of the severity of impact if the risk did occur from a scale of 1 to 5 | Scale of 1 to 5  (Colour automatically assigned by number) |
| RAG (Red / Amber/ Green Status | Score and Colour indicates the total severity and likelihood of the risk | Scale of 2 to 25  (Colour automatically assigned by number) |
| Status change | Indicates change in RAG status since last review date | An arrow pointing up for increased risk, level for no change or down for reduced risk |
| Risk Owner | Indicates person who is responsible/accountable for risk. | Initials of owner |
| Shared risk? | To indicate:  - Whether the risk is shared internally or externally (name of directorate / stakeholder)  - The agreed communication forum  - Any decision made (date / topic) | Free text |
| Relevant Board | To indicate which Board(s) is responsible for reviewing that risk to ensure the risks go to the correct Board and facilitate the work by the PMO. | Name of Board |
| Risk mitigation and intended impact | Indicates the mechanisms and factors that exist to managed the likelihood and impact of risk. | Free text  (New line (alt + enter) for each mitigation) |
| Action owner | Indicates person responsible for managing (investigating and mitigating individual risk) | Initials of owner |
| Due date for actions | Indicates dates by which mitigating actions should be delivered. | dd/mm/yyyy  (ongoing should not normally be accepted) |
| Target residual risk RAG status | Indicates the target RAG score and colour if mitigation is successful | Scale of 2 to 25  (Colour automatically assigned by number) |
| Impacted projects / areas | Explains which projects or areas of business are affected | Free text |
| Escalated? | Indicates if the risk has been escalated | Indicates who, if anyone, the risk has been escalated to |
| Assurance sources | Identifies checking mechanisms that will be used to verify key controls and who will do it | Free text  e.g. SDB / CMG / Internal/External Audit etc. |

# Document Control

**Change Record**

| Version Status | Date of Change | Reason for Change |
| --- | --- | --- |
|  |  |  |
| 2.1 | 01.12.2011 | Approved by HRA Board |
| 2.2 | 05.11.2014 | Updated to include findings from DH internal audit assurance review and HRA internal audit |
| 2.3 | 03.12.2014 | Updated following comments received from CMG / EMT lite |
| 2.4 | 11/01/2014 | Updated with further CMG comments |
|  |  |  |
|  |  |  |
|  |  |  |

**Reviewers**

| Name | Position | Version Reviewed |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Distribution of Approved Versions**

| Name of Person/Group | Position | Version Released |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |