NHS
Counter Fraud Authority

Risk management policy

December 2017

Version 1.0

NHS fraud.
Spot it. Report it.
Together we stop it.

Version control

Version	Name	Date	Comment
Version 1.0	Trevor Duplessis	06/12/2017	First issue.

Document status :	Internal
Document name :	Risk Management Guidance
Author(s) :	Organisational Development / Finance & Corporate Governance
Owner :	Information Governance Lead

Note: Printed copies are only valid on the date they were printed.

Table of contents

1. Introduction

1.1 This policy sets out the overarching approach to managing strategic, project and operational risks within the NHSCFA.

1.2 It should be read by the Board, the Senior Management Team, the Leadership Team and staff who are delegated to manage a specific risk or risks.

1.3 The policy is available for everyone to read on Go2 and the Leadership Team should encourage all staff to become familiar with it.

1.4 The policy is also available to the public on the NHSCFA website.

2. What is 'risk'?

2.1 Risk is defined as the uncertainty of outcome: whether positive opportunity or negative threat, of actions and events1. This means that risks may involve both positive and negative outcomes. An example is given below:

Action	Risks: **Negative**	Risks: **Positive**
A decision is taken to disrupt a criminal organisation through civil litigation rather than spend resources on a full criminal investigation	The action taken may not achieve its objective by failing in court Civil litigation costs may be greater than first thought The decision not to investigate may attract adverse parliamentary comment which may in turn generate adverse media coverage	Resources may be freed up to undertake more productive criminal investigations The civil litigation may succeed and the criminal organisation may stop its activities and may be bound to make reparations Further resources may be obtained in light of a demonstrable shortfall

2.2 Risk management is a fundamental activity and is embedded in our strategic and business planning and project management processes.

[1] HM Treasury, *The Orange Book* (2004). Available from https://www.gov.uk/government/publications/orange-book.

2.3 All risks and opportunities which may have an impact on the achievement of our strategic and operational objectives, or have an impact on individual projects, must be recorded and reported upwards. Both senior management and the Board need to be made aware of these. This will enable them to introduce appropriate measures to manage risks or exploit opportunities.

2.4 Further detailed guidance for internal staff on risk and risk management in the organisation and the completion of the risk register is available on the internal staff intranet.

2.5 Before going on to describe how we as individuals, teams and as an organisation should deal with risk there is another term which is also addressed by this policy. This is ‘issue’. The two terms are often conflated but are quite different.

3. What is an ‘issue’?

3.1 An issue is defined as an event that has happened, or is happening. It is a known as opposed to an unknown quantity.

3.2 The outcome of the actions or events is no longer subject to uncertainty. The consequences may be observed and measured.

3.3 It is possible for one or more of these consequences being identified as actual or potential risks.

4. Risk identification and assessment criteria

4.1 Each work stream will inevitably carry its own risks. These need to be identified, assessed and recorded on the appropriate risk register.

4.2 We currently assess the level of risk by using a simple scoring system based on two criteria:

- Probability
- Impact

4.3 We judge how probable it is that the risk we have identified will lead to an adverse outcome. This is scored on a scale from one to five. See Appendix A below.

4.4 We also judge the likely impact that the adverse outcome might have on our organisation and its ability to meet its strategic and operational objectives. This is scored in a similar way to probability on a scale from one to five. See Appendix B below.

4.5 One further element is also considered in the risk assessment process. Assessing the proximity of the risk informs us of the urgency of the matter and we can incorporate this into our response. To indicate the proximity of an event we use a standard RAG rating. See Appendix C below.

4.6 All identified risks for each work unit are recorded on a risk register. Guidance on how to complete the risk register can be found in the internal guidance document available on the internal staff intranet.

4.7 These individual registers are reviewed and fed into an organisation-wide risk register. This informs the Board and the Senior Management Team of the risks facing the organisation and enables them to respond accordingly.

4.8 Individual stand-alone projects are subject to the same risk identification and management methods set out in this policy. They may be included separately on the organisational risk register if not already included in the risk register for the department in which the project is being developed. Significant risks are reported separately.

4.9 A holistic view of risk concerning our strategic and operational aims allows us to judge whether certain risks might interact with other risks and whether our response needs to reflect this interaction.

4.10 Probability, impact and proximity are dynamic elements and consequently all three must be reviewed and reassessed frequently. This method of identifying, assessing and scoring enables us to prioritise our response.

5. Risk appetite

5.1 Different organisations will have different appetites for tolerating risk. Not all risks can be ‘managed’ out of existence and virtually any significant actions or decisions taken by an organisation, including the conduct of its day to day business carry ‘inherent risks’. The job of risk managers and decision makers is to establish what constitutes a tolerable level of ‘residual risk’ once risk mitigation measures have been taken and are seen to be as effective as anticipated.

5.2 The risk appetite will strongly influence the way a risk is managed. However in order to apply this factor it is necessary to establish the gravity of each risk and prioritise action accordingly.

6. Risk prioritisation

6.1 We give probability and impact a rating from one to five. This allows us to rate each risk, taking into account both criteria. The figure below shows the potential score for each combination of probability x impact.

		Impact				
		1	2	3	4	5
Probability	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

6.2 The greater the probability of the risk coming to fruition and the greater the impact it is likely to have the higher the risk will be rated, and vice versa.

6.3 In line with the scoring system, our general approach to risk is set out below:

- **Extreme risks**, over which we exercise control, are always unacceptable and require a response which will reduce probability or impact or both so that any remaining risk, known as the “residual risk” is reduced to high, moderate or low. Should certain risks be beyond our control there may be occasions where all possible mitigations will still leave the risk score at extreme. These rare instances will be monitored continuously by the Board and Senior Management.

- **High risks** would normally call for mitigation to reduce them to moderate or low. Action taken to mitigate a risk needs to be proportionate to the "cost" of the risk.
- **Moderate risks** may call for mitigation to reduce them to low. Again, such action must be proportionate. An informed decision to tolerate a risk is possible where mitigation would not be cost-effective.
- **Low risks** normally require no further action, unless there is evidence of over - control. Controls incur costs and should not be in place unnecessarily.

7. Risk response

7.1 Risk management and mitigation follows the TRAPS model and may involve one or more of the following:

- **Terminate**

  Where the residual risk after mitigation remains unacceptably high and is beyond the organisation's risk appetite it might be deemed wise to terminate the activity giving rise to the risk. This typically involves the change, removal or abandonment of one aspect of organisational activity.

- **Reduce**

  This means reducing the inherent risk of an activity by reducing the probability of the event occurring or the impact of the event should it occur, or both. This could involve changing the activity giving rise to the risk or finding some way of deadening its impact. Where mitigation action is implemented the success of the mitigation needs to be monitored.

- **Accept**

  This involves a conscious and deliberate decision to retain the threat. This decision may be taken in circumstances where a risk cannot be easily or cost effectively mitigated and where the potential outcome justifies it. This relates to whether the inherent risk is within the organisation's risk appetite.

- **Pass**

  There may be an option open to pass the risk onto a third party who will become responsible for an aspect of the threat. This may be achieved by taking out insurance against an event. However insurance in respect of public bodies may be a restricted option.

- **Share**

  This may involve sharing the risk internally with other parts of the business or with outside organisations or stakeholders.

7.2 Examples of TRAPS measures can be found in the detailed guidance for internal staff available on the internal staff intranet.

7.3 The level of risk remaining after internal control or strategies have been exercised (the ‘residual risk’), should be acceptable and justifiable.

7.4 All actions taken to mitigate or manage risks must be recorded as must the rationale for deciding what level of residual risk may be tolerated.

7.5 The overall process is described in the figure at Appendix D.

8. Roles and responsibilities

8.1 We are all responsible for identifying potential risks and alerting our managers accordingly.

8.2 Some staff may be given responsibility for managing risk in respect of certain work streams or projects. It is important that they familiarise themselves with this policy and the supporting guidance. They will be responsible for reporting on risk to the appropriate member of the Leadership Team who will be the “owner” of the risk.

8.3 Each member of the Leadership Team is responsible for collating the risk register for the risks they own which are reported into the Leadership Team on a monthly basis.

8.4 The Leadership Team is responsible for reporting extreme and high risks and where appropriate interlinked risks to the Senior Management Team and the Board.

8.5 Occasionally reporting risks issues to the Senior Management Team or the Board may require the presence of the risk owner or the person responsible for managing the risk, if different, to elaborate on the risk report.

8.6 Reporting methods, templates and formats can be found in the internal guidance document available on the internal staff intranet.

9. Communication and learning

9.1 All staff have a part to play in contributing to improving the way the organisation manages risk. Risk is a mandatory agenda item in all scheduled team meetings.

9.2 The Leadership Team is responsible for ensuring that effective risk management is communicated appropriately throughout the organisation. Similarly where lessons are learned from less effective risk management practices these should also be disseminated.

9.3 Consideration should be given to highlighting issues to the Corporate Governance Manager & Board Secretary and /or the Information Governance and Risk Management Lead.

10. Reviewing policy and procedures

10.1 This policy and the conduct of risk management processes across the organisation shall be reviewed no less than annually.

10.2 This review should take into account:

- the extent to which all risk owners review the risk controls within the ambit of their responsibility
- the accuracy or otherwise of risk prioritisation by risk owners
- all of the key risks to which the Board have been alerted during the previous twelve months, or shorter period
- any assurance or audit exercises carried out in respect of risk management during the preceding twelve months, or shorter period

Appendix A – Probability matrix

Probability	1	2	3	4	5
Descriptor	**Rare**	**Unlikely**	**Moderate**	**Likely**	**Almost certain**
Frequency: How often might it / does it happen?	This will probably never happen or recur. Not expected to occur for years	Not expected to happen or recur, but it is possible. Expected to occur at least annually	Might happen or recur occasionally. Expected to occur every quarter	Will probably happen or recur, but it is not a persistent issue or circumstance. Expected to occur at least monthly	Will undoubtedly happen or recur, possibly frequently. Expected to occur at least weekly
Probabilities: Will it happen or not?	<0.1%	0.1 – 10%	11 – 30%	31 – 75%	>75%

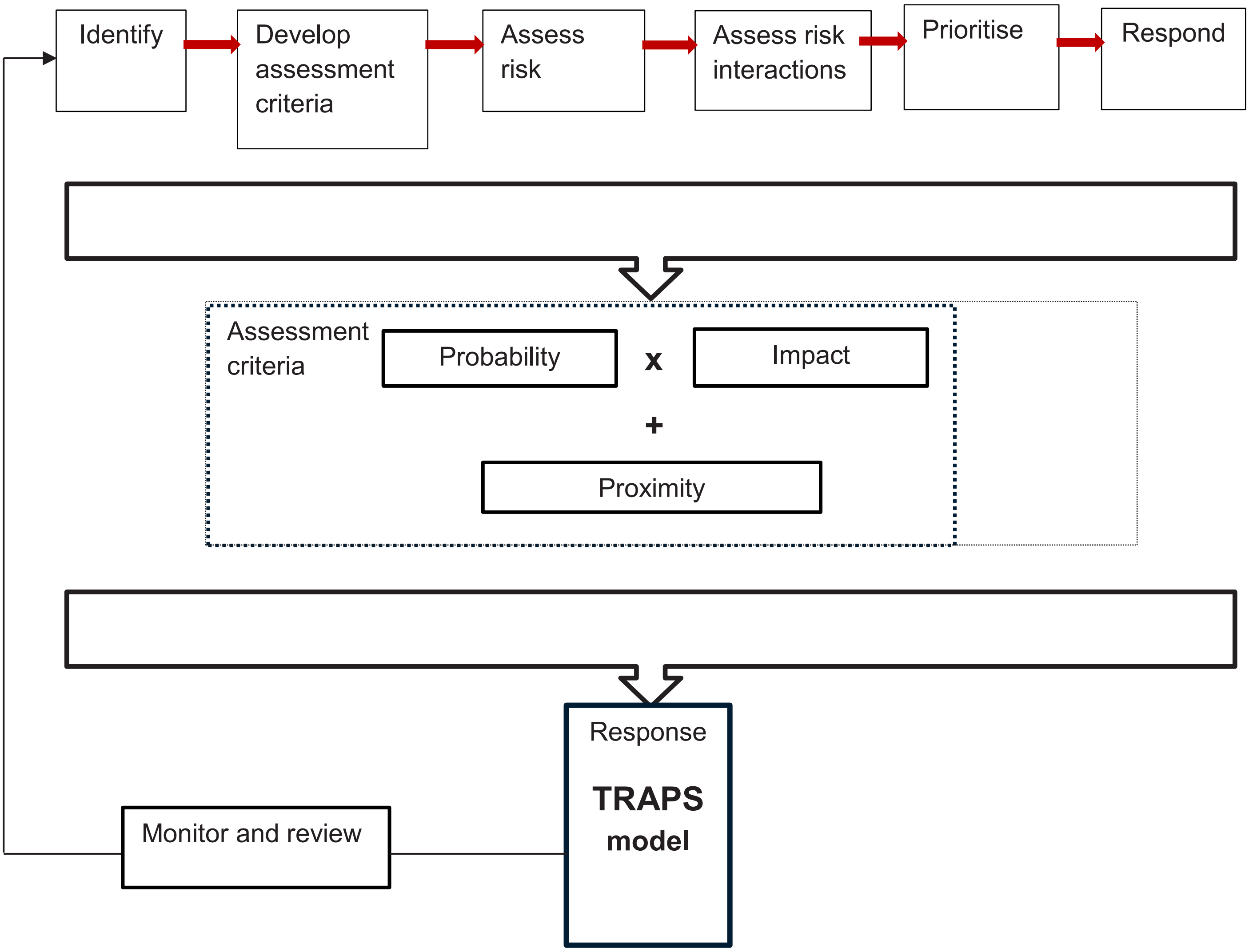
Appendix B – Impact matrix

Impact Level →	Minor 1	Insignificant 2	Moderate 3	Major 4	Catastrophic 5
Business Area ↓					
Cost					
Time					
Quality					
People					
Health & Safety					

Appendix C – Proximity grid

Proximity and timescale for dealing with the risk	**Within one year**	**Within six months**	**Within three months**	**Within one month**	**Within one week**
Descriptor					
Lifecycle / Process	At some stage in the future	Prior to the end of the lifecycle or process	Prior to the end of the next stage or phase	Prior to the end of the next stage or phase	Prior to all other activity being carried out

Appendix D – Overall process


Identify
Develop assessment criteria
Assess risk
Assess risk interactions
Prioritise
Respond
Assessment criteria
Probability
x
Impact
+
Proximity
Response
TRAPS
model
Monitor and review