NHS
Counter Fraud Authority

Risk Management Policy

August 2019

Version: 2.0

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

Version control

Version	Name	Date	Comment
1.0	F&CG	December 2017	Approved
2.0	F&CG	August 2019	Reviewed to reflect the IT application and amendments to the HM Government publication 'The Orange Book' Management of risk - Principles and Concepts

Table of contents

1. Introduction

1.1 This policy sets out the overarching approach to managing risks within the NHS Counter Fraud Authority (NHSCFA).

1.2 It sets out how the NHSCFA will deliver Risk Management across the organisation; outlining who does what and when.

1.3 It should be read by the Board, the Executive Management Team (EMT) Senior Management Team (SMT), the Leadership Team (LT) and staff who are delegated to manage a specific risk or risks.

1.4 The policy is available for everyone to read on the internal staff intranet (Go2) and the Leadership Team should encourage all staff to become familiar with it.

1.5 The Policy is also available to the public on the NHSCFA website.

2. Senior roles and responsibilities

2.1 The NHSCFA Board is responsible for providing strategic leadership for the organisation, ensuring that it is able to account to parliament and the public on how the functions of the NHSCFA are delivered. The Audit Risk Committee (ARC) provides an independent and objective view of the effectiveness of the organisation's internal controls.

2.2 The ARC is responsible for:

- assessing the governance within NHSCFA
- agreeing the Board Assurance Framework (BAF)
- reviewing assurance and governance reports
- reviewing internal audit reports
- reviewing external audit reports; and
- identifying matters to be raised with the Board.

2.3 The NHSCFA's EMT, supported by the SMT provides strategic leadership in all matters relating to the creation and delivery of the organisation's strategy, strategic plans and business priorities.

2.4 The EMT & SMT are responsible for developing the NHSCFA's vision, strategy and strategic plan; setting, agreeing and communicating the annual business priorities to meet the strategic plan.

2.5 The SMT, who meet fortnightly is responsible for:

- setting and overseeing the delivery of the organisation's strategic aims and business priorities
- establishing and maintaining the delivery of governance which includes an effective risk management process and robust internal controls.

2.6 The Leadership Team (LT) provides leadership on the development and delivery of the NHSCFA's strategic plans and business priorities, through the design and implementation of work programmes based on agreed business priorities. It is comprised of the organisation's business leads who meet monthly.

2.7 The LT is responsible for:

- contributing to the development of the strategic plan; and
- providing assurance to the SMT on progress against plans and risks and areas through the identification, mitigation and escalation of risk.

3. What is "risk"?

3.1 Risk is defined as the effect of uncertainty on objectives: whether positive opportunity or negative threat[1]. 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

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

3.2 Risk Management is the co-ordinated activities designed and operated to manage risk and exercise control within an organisation. The proactive identification, classification and control of issues that may affect the NHSCFA's delivery of its objectives. It is a fundamental activity that is embedded in our strategic and business planning and project management processes. Whilst the Board accepts that not all risk can be eliminated, it is committed to reducing its risks to an acceptable level wherever possible.

3.3 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 the EMT, SMT and the Board need to be made aware of these. This will enable them to introduce appropriate measures to manage risks or exploit opportunities.

3.4 Further detailed guidance for internal staff on risk and risk management in the organisation and the completion of the risk register within the Management Reporting Tool application is available on the internal staff intranet[2].

3.5 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.

4. What is an "issue"?

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

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

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

5. Risk Registers

5.1 NHSCFA maintains a single corporate risk register which is overseen by the Board. All entries are reported to the Board and entries scoring 12+ are reported in detail to the ARC. Each work stream will inevitably carry its own risks, which will need to be assessed and recorded and managed via non corporate risk entries. Where there are any risks identified by the LT that could impact upon the NHSCFA, these are discussed together with the Corporate Board Secretary and

[2] Risk Management Guidance

the Risk Management Lead and where appropriate, escalated to SMT to be considered for placement as a corporate risk.

5.2 As the NHSCFA is a relatively small organisation it is practicable to have a single corporate risk register which incorporates both corporate and non-corporate risks and issues. The register is located within the Management Reporting Tool application.

5.3 The risk register contains the following minimum datasets:

Date risk registered	When the risk was first identified
Risk aspect category	The broad general category the risk falls under
Risk description	If [event happens] then [this will be the consequence]
Risk Owner	Named individual who is responsible for the risk
Controls/mitigations	Details the processes in place to control the risk
Inherent risk score	What the current risk score is (probability x impact)
Residual risk score	The anticipated score post mitigation
Lines of defence	1st,2nd and 3rd Lines of defence
Risk response	Terminate/Reduce/Accept/Pass/Share

6. Risk identification and assessment criteria

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

- Probability
- Impact

6.2 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*.

6.3 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*.

6.4 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 Red, Amber Green (RAG) rating. See *Appendix C*.

6.5 All identified risks are recorded on the risk register. Guidance on how to complete the risk register is provided in the internal guidance document available on the staff intranet.

6.6 The non corporate risks are regularly reviewed by the LT and appropriate risks are escalated to a corporate risk on the register. Corporate risks are regularly reviewed by the Risk Register Review Group who recommend actions required to SMT.

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

6.8 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.

7. Risk appetite

7.1 The Board regularly reviews and approves its position on risk appetite. The appetite sets out the level of risk that the NHSCFA is willing to accept. Managers and Team Leads in the organisation are expected to use this to guide their decision making.

7.2 The risk appetite of the NHSCFA is the decision on the appropriate exposure to risk it will accept in order to deliver its strategic objectives.

The NHSCFA's current overall risk appetite is defined as OPEN.

The NHSCFA is willing to consider all potential delivery options to combat fraud and corruption in the NHS in England and the wider health group. Choosing the one, that is most likely to result in successful delivery while also providing an acceptable level of reward and value for money

7.3 Setting the organisation's risk appetite as 'Open'[3] will allow NHSCFA to be innovative in its methods to combat fraud and corruption in the NHS in England, confident that when doing so, it is done in full compliance with its statutory and regulatory obligations.

[3] HM Treasury's: 'Thinking about Risk - Managing your risk appetite: A practitioner's guide'

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

8. Risk Appetite Statement

8.1 The NHSCFA's risk appetite statement is agreed by the Board and the ARC. It is published on the website as a separate document, in addition to being referenced in the annual report. It will cover the overarching areas of:

- Service Disruption
- Legal, Regulatory compliance and Finance
- Personal Information/Bulk Data
- Safety, Health & Environment
- Reputation and credibility
- Technology and cyber threats

8.2 The statement will also define the Board's appetite for each risk.

8.3 Risks throughout the organisation should be managed within the NHSCFA's risk appetite, or where this is exceeded, action taken to reduce the risk.

9. Risk tolerance

9.1 The NHSCFA recognises that in some circumstances it will have to accept a level of risk, in order to achieve its overall objectives. However it must take and accept risks in a controlled manner, thereby reducing its exposure to unacceptable risks.

9.2 NHSCFA uses a standard 5x5 risk scoring matrix (below) for assessing the impact and likelihood of the identified risks. The Board and the ARC have responsibility for monitoring and reviewing all risks scored outside of the organisation's tolerance threshold and taking appropriate action.

9.3 Risk tolerance is the minimum (9+) and maximum risk (12+) that NHSCFA is willing to accept, as outlined in the 'Risk Appetite Statement'. The statement details risk categories against which all identified organisational unit risks are assessed for their likelihood and impact using the 'probability and impact' scoring matrix.

9.4 Any risks rated at or above the minimum score are reported to the Business Unit Leads on a monthly basis. A risk score of (9+) is treated as a trigger for a discussion at the Leadership Team (LT) meeting, together with Board Secretary and the Risk Management Lead, to determine whether the risk score is justified. Any risks considered to be correctly rated will be escalated to the SMT for review and to be actioned accordingly.

9.5 A target risk rating should be set for all risks. This target (the “residual”) risk rating is a means of expressing a target for the lowest acceptable (“tolerated”) level for that risk. When setting residual risk ratings, risk leads should consider what level of tolerated risk they are willing to retain. For some risks, the residual risk rating could be high, especially where the consequences are potentially severe or some elements of the risk lie outside the direct control of the business unit or organisation.

9.6 The ARC supports the Board by reviewing among others, the comprehensiveness and reliability of assurances on governance and risk management. The ARC will have sight of all Corporate risks scoring (12+).

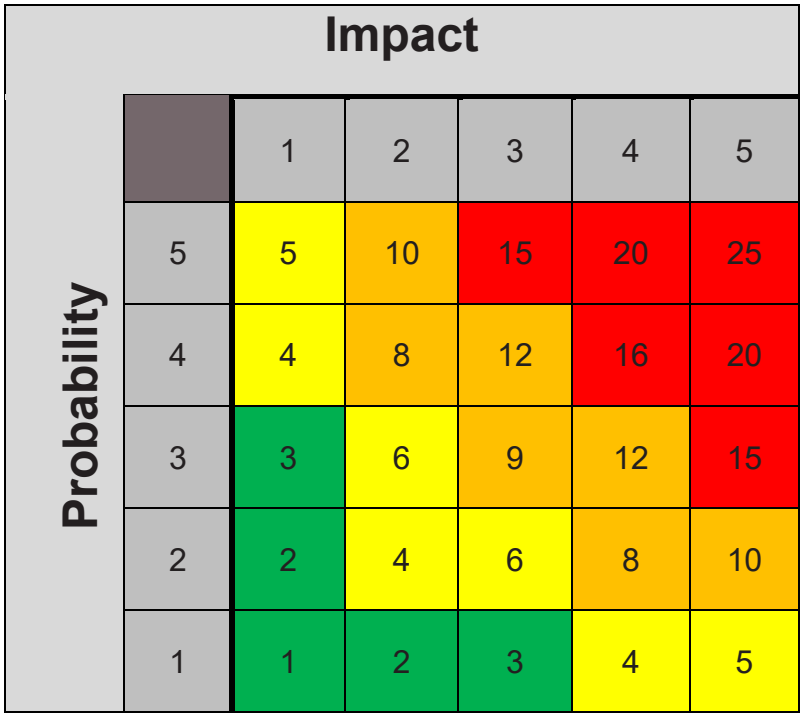
9.7 The Board will review the position on risk appetite at least annually against any new NHSCFA strategic objectives and will produce an annual statement of risk appetite.

10. Risk prioritisation

10.1 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.

10.2 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.

10.3 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.



10.4 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*.

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

10.5.1 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 the SMT.

10.5.2 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.

10.5.3 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.

10.5.4 LOW risks normally require no further action, unless there is evidence of over - control. Controls incur costs and should not be in place unnecessarily.

11. Assigning a risk score

11.1 As part of the risk assessment process, each identified risk should undergo a three stage evaluation process.

11.1.1 'Inherent' - review as though there were no controls in place or the proposed controls in place are failing; then

11.1.2 'Residual' - assume adequate controls are in place and are operating effectively; and now

11.1.3 'Set a Score' - this is achieved by implementing action to bring the risk in line (where possible) with the articulated appetite and tolerance level.

11.2 The table below may assist in helping to set an appropriate score for the risk:

Risk Rating	Risk	Action Required	Minimum Review
1-8	LOW	ACCEPT RISK Manage by routine procedures and existing policies/guidance	To be review every 6 Months by nominated actionee/Risk Lead
8-12	MEDIUM	SMT/LT MANAGEMENT ACTION REQUIRED Costs to be funded within Business Unit. May necessitate bid for Central funding	To be reviewed monthly by the nominated actionee/Risk Lead To be discussed/reviewed at the LT Meeting re potential escalation.
12-25	HIGH	Board/ARC Action Required Board to be informed of priority funding	To be reviewed every 3 months by the nominated Board/SMT actionee/Risk Lead To be discussed and reviewed by the ARC

12. Escalating risks

12.1 Risks are scored so that they can be prioritised for action. Risk management should be proportionate to the level of risk and the NHSCFA will focus resources on addressing those risks with the greater probability of coming to fruition. The greater the impact it is likely to have the higher the risk will be rated and vice versa.

12.2 Escalation is about informing the organisation and mobilising additional resources to mitigate the risk, particularly where local resources are insufficient. At the business unit level, Team Leads should assess the risk to the team objective, articulated in their unit business plan.

12.3 Where a business unit risk has arisen that the risk owner is concerned might impact on the strategic objective(s) of the organisation, this will be raised for discussion at the LT meeting together with the Board Secretary and Risk Management Lead. Where it is decided that a business unit risk should be escalated to the SMT for consideration, this will be done via the Board Corporate Secretary.

12.4 Escalation to the corporate risk register will be based on the following criteria:

- the risk score is equal to or higher than (12) or
- the Risk Management Lead has reported a thematic risk having identified similar risks across the organisation (e.g. a workforce issue).

13. Opportunity risks

13.1 There can be a danger when the organisation focuses on negative risks, that it will sometimes forego opportunities that while initially appearing to be too risky, have never been formally analysed. While positive risk is something the organisation will generally want to avoid, when they do occur it can often be managed as an opportunity and therefore it is equally important to prioritise actions and to concentrate on those opportunities that are most likely to bring about a successful outcome.

13.2 When deciding whether to take an opportunity risk ('treat' the opportunity), the same principles apply. The costs involved in exploiting the opportunity must be justifiable in terms of the anticipated benefits and the controls should not lead to significant risks.

13.3 Risk appetite levels will depend on the circumstances; for example NHSCFA will have a low tolerance to taking risks which may severely impact on the security and integrity of its information systems, but may have more appetite for opportunity risks such as major IT service developments which while presenting significant challenges, will ultimately bring benefits to the organisation.

13.4 The risk responses for opportunity risks are similar to those for negative risks and are categorised as follows:

13.4.1 **Exploit**

Ensuring the opportunity is realised.

13.4.2 **Escalate**

Where an opportunity arises that a business unit is unable to realise as they lack the requisite authority to take the necessary step.

13.4.3 **Enhance**

Increase the chance of the risk happening so that the benefits of the opportunity can be realised.

13.4.4 **Accept**

No action is taken to realise the opportunity; it is left as it is and if it happens on its own, then the organisation will benefit from it (mainly used when the cost of the response is high and there is less chance of it occurring or the benefit does not outweigh the effort involved).

13.4.5 **Share**

This is where a business unit is not capable of realising the opportunity on its own and so works together with another business unit or stakeholder to realise the opportunity.

14. Corporate risks

14.1 The Board will be responsible for the monitoring and of all corporate risks via the Risks & Issues overview report The Risk Management Lead will be responsible for gatekeeping and assurance checking to ensure the appropriateness of risks on the register. Challenges will be raised via the Risk Register Review Group.

14.2 The ARC will have responsibility for reviewing the corporate risks via the BAF Risks & Issues report.

14.3 The Board Secretary will be responsible for adding any new strategic risks to the BAF risk & issues report or amending any previous risks.

15. Risk response

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

15.1.1**Terminating**

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.

15.1.2 **Reducing**

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.

15.1.3 **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.

15.1.4 **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.

15.1.5 **Share**

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

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

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

15.4 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.

15.5 The overall process is described in the figure at Appendix D

16. Staff roles and responsibilities

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

16.2 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.

16.3 Each member of the Leadership Team is responsible for collating the risks they own which are reported to the Leadership Team meetings on a monthly basis.

16.4 Occasionally, reporting risk issues to the SMT, Board or ARC may require the presence of the risk owner or the person responsible for managing the risk if different, to elaborate on the risk report.

17. Communication and Learning

17.1 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.

17.2 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.

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

18. Reviewing policy and procedures

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

18.2 This review should take into account:

18.2.1 The extent to which all risk owners review the risk controls within the ambit of their responsibility;

18.2.2 The accuracy or otherwise of risk prioritisation by risk owners

18.2.3 All of the key risks to which the Board/ARC have been alerted during the previous twelve months, or shorter period

18.2.4 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

Appendix B

Impact Matrix

Impact Level	**1**	**2**	**3**	**4**	**5**
Descriptor	**Minor**	**Insignificant**	**Moderate**	**Major**	**Catastrophic**
Risk Aspect					
Service Disruption					
Legal, Regulatory Compliance & Finance					
Personal Information/Bulk Data					
Safety, Health & Environment					
Reputation & Credibility					
Technology and Cyber Threats					

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