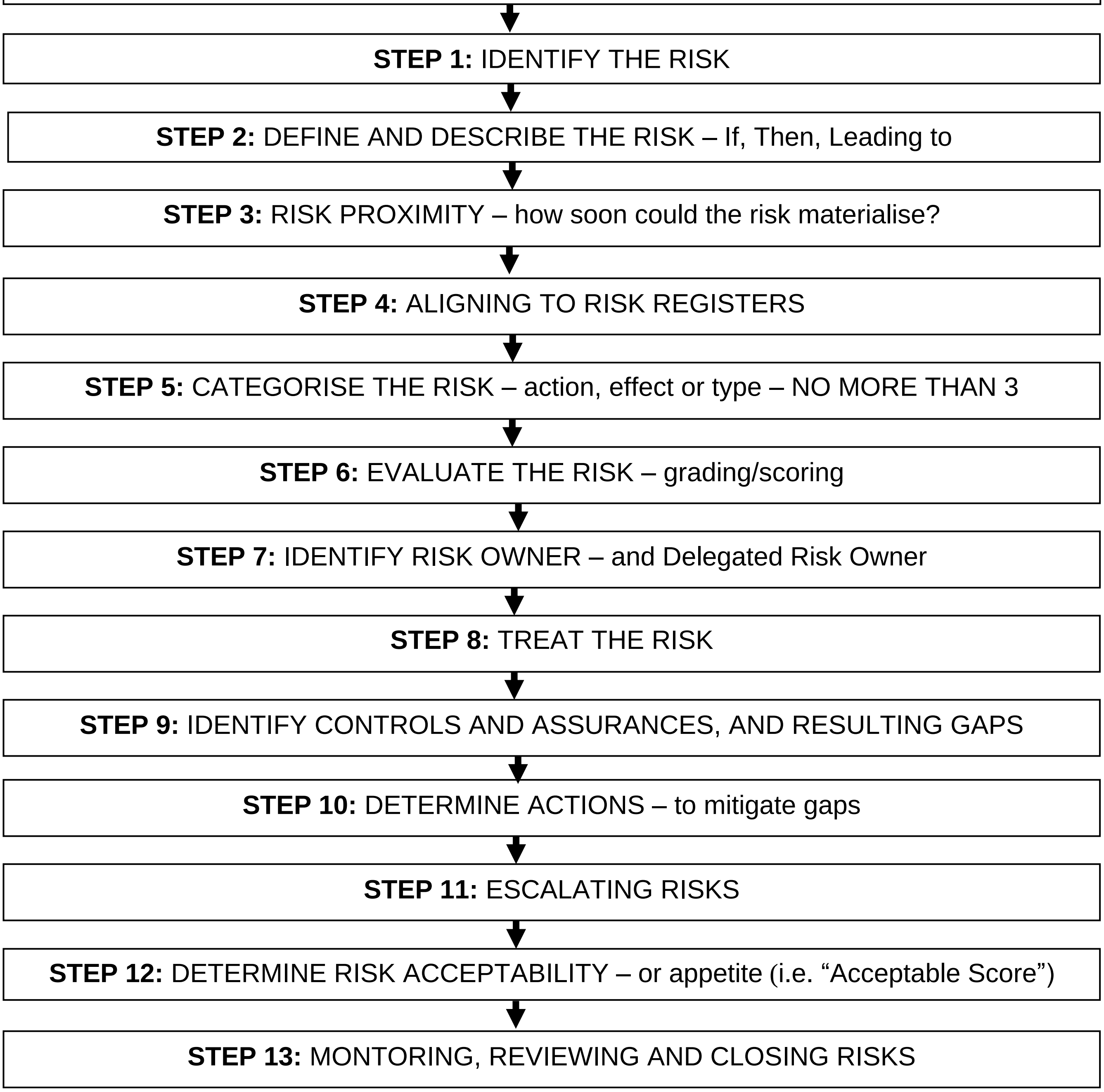
NHS
Buckinghamshire
Clinical Commissioning Group

Risk Management Flowchart



STEP 1: IDENTIFY THE RISK

STEP 2: DEFINE AND DESCRIBE THE RISK – If, Then, Leading to

STEP 3: RISK PROXIMITY – how soon could the risk materialise?

STEP 4: ALIGNING TO RISK REGISTERS

STEP 5: CATEGORISE THE RISK – action, effect or type – NO MORE THAN 3

STEP 6: EVALUATE THE RISK – grading/scoring

STEP 7: IDENTIFY RISK OWNER – and Delegated Risk Owner

STEP 8: TREAT THE RISK

STEP 9: IDENTIFY CONTROLS AND ASSURANCES, AND RESULTING GAPS

STEP 10: DETERMINE ACTIONS – to mitigate gaps

STEP 11: ESCALATING RISKS

STEP 12: DETERMINE RISK ACCEPTABILITY – or appetite (i.e. “Acceptable Score”)

STEP 13: MONTORING, REVIEWING AND CLOSING RISKS

STEP 1: IDENTIFY THE RISK

a) Source
Methods for identifying and managing levels of risk would include:

- Member practices
    - ✓ Practice visits
    - ✓ Locality Meetings
    - ✓ Accountability Forums
    - ✓ Patient Participation Groups
    - ✓ Patient engagement forums
    - ✓ Practice feedback forums
    - ✓ Practice Managers meetings.
- Internal methods, such as; Incidents, complaints, claims and audits, project risks based on the achievement of project objectives, patient satisfaction surveys, risk assessments, surveys including staff surveys, whistle-blowing. Contract quality monitoring of commissioned services. Also via various internal processes and monitoring arrangements including:
    - ✓ Strategic planning
    - ✓ Operational Planning operational planning
    - ✓ Programme and project management
    - ✓ Quality and Performance Reports
    - ✓ Internal Audits
    - ✓ Risk assessment
    - ✓ CCG Committees and sub committees
    - ✓ CCG Membership
    - ✓ Staff members
    - ✓ Staff surveys
    - ✓ Patient satisfaction surveys
    - ✓ Serious Incidents
    - ✓ Incidents and complaints monitoring
    - ✓ Claims
    - ✓ Health and Safety, Fire and Environmental audits
    - ✓ Training needs analysis
- External methods, such as; Media, national reports, new legislation, surveys, reports from assessments/inspections by external bodies, reviews of partnership working, or via various pathways and agencies, including external assessments and inspections:
    - ✓ NHS England
    - ✓ National reports and guidance
    - ✓ NHS Litigation Authority
    - ✓ Health and Safety Executive
    - ✓ External audit
    - ✓ Care Quality Commission inspections
    - ✓ Ombudsman reports
    - ✓ Central Alerting System (CAS) from Department of Health
    - ✓ Partner agencies
    - ✓ Commissioned providers
    - ✓ Coroner reports
    - ✓ Media and publications
    - ✓ National Patient Safety Agency alerts
    - ✓ Medicines and Healthcare products Regulatory Agency

Risks will generally be identified by individuals against a defined aim/goal/objective, these include:

- Strategic aims/goals or Operational Plan (Corporate Risks)
- Project / Programme delivery (Programme Risks)
- Functional team / Service (Project or Programme Risks)
- Adverse feedback – quality issue, audit or review (Project or Programme Risks)

Project or programme risks can be identified and mapped to Verto by any individual aligned to a project or programme in the first instance and against one or more categories of risk (step 5). Only after this has been undertaken will a risk be assessed at corporate risk level.

STEP 2: DEFINE AND DESCRIBE THE RISK – If (cause), then (effect), leading to

A risk should use the following method of best practice to best define it

IF (i.e. what is the risk) – e.g. increase in activity more than expected, increase in infection rates beyond trajectory
THEN (i.e. what might happen if it materialises) – e.g. related target will not be met, trajectory breach, patient harm
LEADING TO: (i.e. further consequences for the CCG) – e.g. non-compliance with statutory duty/loss of income/quality premium, poor outcomes, poor patient experience/reputation, additional stakeholder scrutiny (e.g. NHS E quarterly assurance)

Risk definitions can otherwise be misplaced. If we use the Accident and Emergency waiting time target of 95% within four hours as the example:

Table 1: Misplaced definitions of risk

A wrong description…	**What is not a well-defined risk…?**
Failure of an objective	Not seeing patients within four hours of their arrival
Success of an objective	Seeing all patients within four hours
Composite risk	Patients won't be seen within four hours because there are not enough consultants in the department
One word risks	Reputation
Statement of fact	There is a risk the department won't meet the target
Failure to	Failure to meet the waiting time target
Incident	Due to ambulance handover delays the waiting time target will not be met
Issue	Because there aren't enough consultants in the department, the target can't be met
Whinge	Cuts to budgets and lack of interest in vacant posts has created extra work for the consultants left which means reduced capacity and likelihood that the target can't be met
Essay	A whinge and more

It's also important to focus the risk on the impact on the CCG and not the provider, and also not focus individual risks on individual providers where possible and especially at corporate risk level.

So what's the answer?
IF (what is the risk) providers do not meet the 95% waiting time target by end of the financial year.
THEN (what happens if it materialises) the NHS constitution standard will not be met
LEADING TO (further consequences for the CCG) increased scrutiny from NHS England through quarterly assurance and increased risk of financial penalty through non-achievement of quality premium.

A Risk ID will appear automatically when a new risk is entered. A “date identified” will also need to be inserted.

Risk Title = IF (what is the risk)
Description = THEN (what happens if the risk materialises), LEADING TO further consequences for the CCG
Risk Cause = source of the risk. Using the A&E example this could read “increasing demand on accident and emergency through an increasingly elderly population and staff shortages”. This picks up some of the related factors associated with the risk, but does not include them in the definition/description.

STEP 3: RISK PROXIMITY – how soon could the risk materialise?

Risk proximity means how far away in time will the risk occur (if it materialises), it can also mean when the risk will occur.   Risk proximity helps us focus on certain risks that may occur soon, and ignore risks that cannot occur in the near future. This will make risk management more efficient. Verto options for Risk Proximity (which will affect choice of Risk Review date)

Table 2: Risk proximity options and next review dates

Risk proximity option	**Next review date**
Immediate	1 month (i.e. next meeting of board or project which manages the risk)
0-3 months	1 month (i.e. next meeting of board or project which manages the risk)
3-6 months	2-3 months’ time
More than six months	3-4 months’ time

STEP 4: ALIGN TO RISK REGISTERS

Risk Registers are used to organise and manage risk at project/team and corporate risk levels. A Risk Register is a risk management tool which acts as a central repository for all risks identified by the organisation or project. For each risk the register will include information such as risk likelihood, impact, the actions to be taken, the Risk Owner and so on. Managers should view the risk register as a management tool to review and update the process that identifies, assesses, and manages risks down to acceptable levels. Actions are then instigated to reduce the probability and the potential impact of specific risks.

For the list of risk registers on which risks can appear, please refer to section 5.1 of the Integrated Risk Management Framework.

In respect of a risk appearing on the Corporate Risk Register (CRR) or Governing Body Assurance Framework, escalation will be based on following the process described in step 12. A Risk Owner (see step 7 for a definition) at project or team level would not be expected to undertake any re-assessment to agree a corporate risk grade/score. Each new risk entered on Verto can be aligned only to one Risk Register from the above list, excluding the Corporate Risk Register and Governing Body Assurance Framework (GBAF).

STEP 5: CATEGORISE THE RISK – Action, Effect or Type

Risks can be categorised in a number of different ways:

(1) In terms of the level of action required to mitigate the risk– e.g. immediate due to high risk through to no action required where risk is low
(2) In terms of their effect or consequence, E.g. financial or reputational
(3) In terms of their alignment to a strategic aim/goal.
(4) In terms of their type, i.e. the area of business to which they relate – e.g. Finance, Information Governance, performance etc.

It is method 4 which is specifically used to categorise risks in Verto. To ensure consistency in application of risk categories, risk registers may be subject to comparison and cross reference before, during and after escalation and de-escalation of risks from the corporate risk register.

Table 3: Verto risk categories

Verto category	**Comments/examples**
Business Continuity	Includes winter resilience
Strategic Aim/Goal	See above listing
Performance/contracts	E.g. gap in control or assurance, CPN
Procurement	E.g. delay to process/timescale
Contracts issues (excluding performance and quality)	E.g. sign off past long stop
Corporate	Includes Health and Safety
Finance	E.g. future costs unclear/unallocated QIPP
Human Resources	E.g. CCG vacancies, Loss of key staff without notice
Organisational Development	E.g. Loss of key staff without notice
Sustainability	E.g. CSU relationships, sickness relates
Patient Experience	E.g. poor evidence of engagement
Quality	Associated with Darzi domains. Includes any issues related to Quality Impact Assessments (QIA)
Safeguarding	E.g. non-compliance with training rates or legislation
Best clinical practice e.g. NICE, Francis, Keogh, Berwick	i.e. non-compliance with by providers
Clinical Governance	E.g. clinical concerns process issues
Reputation	E.g. lack of agreement between commissioners on funding arrangements
Equality and Diversity	E.g. non-compliance with nine protected characteristics. Includes any issues related to Equality Impact Assessments
Safety	E.g. non-compliance with trajectories for Healthcare Acquired Infections (HCAI)
Medicines Management	E.g. gender dysphoria
Information Governance	Includes any issues related to Privacy Impact Assessments. E.g. non-compliance with IG toolkit, IG breaches through data loss
Constitutional targets	Any risk affecting quality premiums
Corporate Governance	E.g. Conflicts of interest, legislation, claims
Financial Governance	E.g. bribery and corruption
Primary Care/delegated responsibility	E.g. members not voting for delegated commissioning

STEP 6: EVALUATE THE RISK – grading/scoring

Documented risk and assessment (evaluation) are essential to enable the CCG to:

- Identify risk priorities, in particular the most significant risk issues
- In parallel with the risk registers, capture decisions about what is and what isn't acceptable risk
- Provide a consistent record of the way in which risk is addressed
- Facilitate the review and monitoring of risks

Risk falls into three components:

- The baseline risk – before any controls are put in place
- Risk mitigation – management controls, assurances and actions
- Current risk – after controls, assurances and actions have been implemented

An evaluation matrix provides a method of quantifying risk by defining measures of likelihood (frequency or probability) and consequence (severity) using a 1 to 5 rating system. The higher the risk level, the greater the likelihood an opportunity or threat will occur and the greater its consequence.

The resulting score (from 1 to 25) result in the grading of risks from Low (Green) to Extreme (Red). It is therefore important to use a process that measures impact and likelihood consistently and enables the development of a hierarchy of risk for the registers.

<u>Table 4: Risk Ratings</u>

Rating	**Score**	**Comments**
Red	12-25	Extreme and unacceptable. The consequences of these risks could seriously impact on the organisation's objectives and the responsible Director should ensure that there are suitable and sufficient action plans in place to reduce the risk and that strategic risks are escalated to the Governing Body Assurance Framework (GBAF). It is the responsibility of the relevant manager to inform the Accountable Officer and a nominated director if there is any delay in mitigating the risk. Treatment action plans and acceptability for high risks are monitored by the Executive Committee and are reported to each meeting of the Governing Body for consideration and action as deemed necessary.
Orange	8-10	High risk and unacceptable. These should be reported on the Corporate Risk Register (CRR). With a concerted effort (for example extra resource in terms of funding, staff time etc.) and a challenging action plan, these risks could be realistically reduced within the required timescale. Managers or staff who identify risks to be 'high', should bring them to the attention of the Risk Owner or Head of Service immediately, who will be responsible for adding the risk to Verto, taking advice where necessary from a Director and the Corporate Governance Lead.

Rating	Score	Comments
Yellow	4-6	These are considered “moderate risk” and are tolerable provided the appropriate responses are in place to minimise the likelihood of undesirable occurrences. It should be realistically possible to reduce these risks within a reasonable timescale through reasonably practicable measures to mitigate them. Existing responses should be reviewed, with regular auditing of their effectiveness undertaken. It is the responsibility of relevant managers to ensure that the risk register is kept up-to-date, reviewed at meetings, with relevant actions taken in order to monitor and mitigate all moderate risks. Risks scored as moderate are deemed acceptable and therefore need to be controlled /reduced or the activity or development stopped.
Green	0-3	These are low risk and would probably be unlikely to occur. These risks are regarded as acceptable and should be managed locally or within the relevant directorate areas. Projects should review low risks on a regular basis at relevant meetings and mitigate through application of relevant and proportionate controls, assurance and actions. Managers or Team Leaders who are responsible for managing these risks, should take advice where necessary, from the Corporate Governance Lead if trends or patterns have been identified in risk assessments. It is the Manager, Risk Owner or Delegated Risk Owners responsibility to enter these risks into their project or programme risk registers. The Risk Owner/Delegated Risk Owner should make decisions on a monthly basis which Low level risks should be archived if no action is required to mitigate these risks. These risks once fully mitigated can be archived and also, retrievable if need be.

Risk evaluation - likelihood

Consequence	**A measure of the e risk occurring**	**Catastrophic**	**5**	**10**	**15**	**20**	**25**
		Major	**4**	**8**	**12**	**16**	**20**
		Moderate	**3**	**6**	**9**	**12**	**15**
		Minor	**2**	**4**	**6**	**8**	**10**
		Insignificant	**1**	**2**	**3**	**4**	**5**
Likelihood Measure of the probability that the predicted harm, loss or damage will occur.			**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
			Extremely unlikely. *May* only occur in exceptional circumstances. Has never occurred before.	Unlikely to occur/recur, but possible. Occurred less than once per annum.	May occur/recur, but not definite. Has previously occurred once or twice per annum.	Will probably occur/recur. Has happened several times per annum before.	Continuous exposure to risk. Has happened before regularly and frequently.
Frequency How often night it happen?			Not expected to occur for years	Expected to occur at least annually	Expected to occur at least monthly	Expected to occur at least weekly	Expected to occur at least daily
Probability			<1%	1-5%	6-20%	21-50%	>50%
			Will occur only in exceptional circumstances	Unlikely to occur	Reasonable chance of occurring	Likely to occur	More likely to occur than not

	Consequence score (severity levels) and examples of descriptors				
	1	**2**	**3**	**4**	**5**
Domains	**Insignificant**	**Minor**	**Moderate**	**Major**	**Catastrophic**
Impact on the safety of patients, staff or public (physical/psychological harm)	Minimal injury requiring no/minimal intervention or treatment. No time off work	Minor injury or illness, requiring minor intervention Requiring time off work for >3 days Increase in length of hospital stay by 1-3 days	Moderate injury requiring professional intervention Requiring time off work for 4-14 days Increase in length of hospital stay by 4-15 days RIDDOR/agency reportable incident An event which impacts on a small number of patients	Major injury leading to long-term incapacity/disability Requiring time off work for >14 days Increase in length of hospital stay by >15 days Mismanagement of patient care with long-term effects	Incident leading to death Multiple permanent injuries or irreversible health effects An event which impacts on a large number of patients
Quality/complaints/audit	Peripheral element of treatment or service suboptimal Informal complaint/inquiry	Overall treatment or service suboptimal Formal complaint (stage 1) Local resolution Single failure to meet internal standards Minor implications for patient safety if unresolved Reduced performance rating if unresolved	Treatment or service has significantly reduced effectiveness Formal complaint (stage 2) complaint Local resolution (with potential to go to independent review) Repeated failure to meet internal standards Major patient safety implications if findings are not acted on	Non-compliance with national standards with significant risk to patients if unresolved Multiple complaints/ independent review Low performance rating Critical report	Totally unacceptable level or quality of treatment/service Gross failure of patient safety if findings not acted on Inquest/ombudsman inquiry Gross failure to meet national standards

	Consequence score (severity levels) and examples of descriptors				
Human resources/ organisational development/staffing/ competence	Short-term low staffing level that temporarily reduces service quality (< 1 day)	Low staffing level that reduces the service quality	Late delivery of key objective/ service due to lack of staff Unsafe staffing level or competence (>1 day) Low staff morale Poor staff attendance for mandatory/key training	Uncertain delivery of key objective/service due to lack of staff Unsafe staffing level or competence (>5 days) Loss of key staff Very low staff morale No staff attending mandatory/ key training	Non-delivery of key objective/service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several key staff No staff attending mandatory training /key training on an ongoing basis
Statutory duty/ inspections	No or minimal impact or breech of guidance/ statutory duty	Breech of statutory legislation Reduced performance rating if unresolved	Single breech in statutory duty Challenging external recommendations/ improvement notice	Enforcement action Multiple breeches in statutory duty Improvement notices Low performance rating Critical report	Multiple breeches in statutory duty Prosecution Complete systems change required Zero performance rating Severely critical report
Adverse publicity/ reputation	Rumours Potential for public concern	Local media coverage – short-term reduction in public confidence Elements of public expectation not being met	Local media coverage – long-term reduction in public confidence	National media coverage with <3 days service well below reasonable public expectation	National media coverage with >3 days service well below reasonable public expectation. MP concerned (questions in the House) Total loss of public confidence
Business objectives/ projects	Insignificant cost increase/ schedule slippage	<5 per cent over project budget Schedule slippage	5–10 per cent over project budget Schedule slippage	Non-compliance with national 10–25 per cent over project budget Schedule slippage Key objectives not met	Incident leading >25 per cent over project budget Schedule slippage Key objectives not met
Finance including claims	Small loss Risk of claim remote	Loss of 0.1–0.25 per cent of budget Claim less than £10,000	Loss of 0.25–0.5 per cent of budget Claim(s) between £10,000 and £100,000	Uncertain delivery of key objective/Loss of 0.5–1.0 per cent of budget Claim(s) between £100,000 and £1 million Purchasers failing to pay on time	Non-delivery of key objective/ Loss of >1 per cent of budget Failure to meet specification/ slippage Loss of contract / payment by results Claim(s) >£1 million
Service/business interruption Environmental impact	Loss/interruption of >1 hour Minimal or no impact on the environment	Loss/interruption of >8 hours Minor impact on environment	Loss/interruption of >1 day Moderate impact on environment	Loss/interruption of >1 week Major impact on environment	Permanent loss of service or facility Catastrophic impact on environment

Before completing a grade/score for the risk following evalaution, Verto requires a ratification for this evaluation. On what basis has the evaluation been reached? Why a particular level of impact and likelihood and not any other?

Reasoning for baseline Score/Reasoning for current Score
This gives an opportunity to further explain why a specific score has been given as opposed to any other, in additional to the level of explanation that is already given by choice of score for likelihood and impact.

Example:
IF (what is the risk) providers do not meet the 95% waiting time target by end of the financial year.
THEN (what happens if it materialises) the NHS constitution standard will not be met
LEADING TO (further consequences for the CCG) increased scrutiny from NHS England through quarterly assurance and increased risk of financial penalty through non-achievement of quality premium.

Reasoning for Baseline Score (at 1 April) (5X5 = 25): likelihood of high impact and high likelihood already known because the same target has not been met in previous years.

(Assuming for this example that this reasoning is given at Month 10, January) Reasoning for Current Score (5X5 = 25): performance year to date has been at below 95% and therefore chances of this risk materialising remains high and highly likely.

A committee being assured on this risk would not necessarily know this from the current score given – this box offers the opportunity to further explain it.

Completion is not explicitly necessary, though it is the role of the responsible committee/meeting/group determine whether this should be completed or not depending on its level of expected assurance.

Additional note:

For any risk that is entered onto Verto, there is a requirement to enter both baseline and current scores through the field entitled “Project Likelihood & Consequence after Controls & Assurances have been put in place”.

As this is a standard field, it is does not change its name where the risk being entered relates to a programme and not a project, and where the risk is then aligned as a non-project related risk.

The user can therefore safely and correctly assume that the baseline and current scores are programme level. In the same manner as project level risk escalation, Programme level risks scored 12-25 will also need to be moderated by the Executive Committee to agree a corporate risk score which is then added to the risk.

The current score given should be based on what has already been delivered, not where this risk is expected to be once actions have been delivered.

Question:

Reasoning for baseline score (to explain why a risk has a certain score) is clear, but is "reasoning for current score" box really necessary? Would this not already be clear from the impact and likelihood score already given for the risk?

Possibly, but this will depend on the timescale over which the risk has been defined and proximity of the risk occurring. For example: IF acute providers did no not meet A&E waiting time target of 95% by 31 March (baseline 1 April) and the current score measure is at mid-point through the year. Baseline and current score are both scored 5x5 (i.e. despite controls, controls and assurances), chances of the risk materialising remain high. That would be known from the current score, but the box could then explain why - e.g. because the cumulative average in the first 6 months is 85% and that is why the risk will likely materialise by 31 March. This trend may or may not be known if it is not explained in the box.

STEP 7: IDENTIFY RISK OWNER – and Delegated Risk Owner

Risk Owner	The individual who is responsible for the management and control of all aspects of individual risks. These individuals are responsible for managing risk locally and for ensuring that the risks are reviewed at least monthly and escalated where necessary. They are responsible for taking a lead role in embedding risk management processes within their project/team. This is not necessarily the same as the action owner, as actions may be delegated to others. They are specifically responsible for: • Ensure local risk registers are maintained and updated • Ensure risks that meet the tolerance level of 8 or more are escalated to either the Corporate Risk Register or Governing Body Assurance Framework • Providing assurance on risk management activity through the relevant Board/Group/Partnership/Forum/Committee to which the project or team is ultimately accountable. Depending on the risk and the register to which it is assigned, a Risk Owner (at project level) should always be: • The Senior Responsible Officer (SRO) for the project • A managerial deputy to a Clinical Commissioning Director or Clinical Lead, • Deputy to a senior manager that is a member of the Governing Body and/or Executive Committee, • Another manager with risk responsibility as part of portfolio, e.g. Project Manager or Locality Business Support Manager.
Delegated Risk Owner	The individual often responsible for populating and updating project or team Risk Registers, Board/Group/Partnership/Forum/Committee Risk Registers and those associated with Regulatory and Corporate Affairs through the Verto system. The roles and responsibilities of these individuals include: • Proactively engage in reviewing monthly risk reports/ registers and update within their project/team. Delegated Risk Owners should work with Risk Owners to ensure registers are quality checked. • Input risk information on to the Verto system in an accurate and timely manner to enable production of Risk Reports. • Keep up to date with any changes to the risk management software system by attending refresher training as and when appropriate. • Report any concerns to their Director and advise directors, managers and other staff within their team of identified risks requiring attention.

	Depending on the risk and the register to which it is assigned, a delegated risk owner should always be: (1) A managerial deputy to a Senior Responsible Officer (SRO) for the project, managerial deputy to a Clinical Commissioning Director or managerial deputy to a Clinical Lead, (2) Deputy to a senior manager that is a member of the Governing Body and/or Executive Committee, (3) Another manager with risk responsibility as part of portfolio, e.g. Project Manager or Locality Business Support Manager. This individual may be responsible (as deputy to the risk owner) for reviewing and updating risks through the Verto system.

Table 5: Risk proximity options and next review dates

Risk proximity	**Next review date**
Immediate	1 month (i.e. next meeting of board or project which manages the risk)
0-3 months	1 month (i.e. next meeting of board or project which manages the risk)
3-6 months	2-3 months' time
More than six months	3-4 months' time

STEP 8: TREAT THE RISK

Before deciding controls, assurances and actions (steps 9 and 10), decisions need to be taken on how to respond to each risk. The choice of method to treat the risk (and resulting controls, assurances and actions) will also depend on the acceptable score identified.
The responses to the risk should be one of the following:

ACCEPT (otherwise referred to as **TOLERATE**)
The exposure may be tolerable without any further action being taken or you may have reduced your risk as far as possible. Even if it is not acceptable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to any benefit gained. This risk can therefore remain on a Risk Register, but it is advisable to have in place contingency planning for handling any impacts that could arise if the risk is realised.

AVOID (otherwise referred to as **TERMINATE**)
Some risks will only be treatable or containable to acceptable levels by terminating the activity. Thought should always be given to tackling an objective and doing something differently thus removing the risk but only if it is either feasible or practical to do so. This option can be particularly important in project management if it becomes clear that the projected cost/benefit is in jeopardy.

EXPLOIT
This option should be considered whenever accepting, transferring or reducing a risk. There are two aspects to this. The first is whether or not at the same time as mitigating threats an opportunity arises to exploit positive impact. For example, if a large sum or capital funding is to be put at risk in a major project, are the relevant controls judged to be good enough to justify increasing the sum of money at stake to gain even greater advantages? The second is whether or not circumstances arise which, whilst not generating threats, offer positive opportunities. For example, a drop in the cost of goods or services frees up resources which can be redeployed.

REDUCE *(otherwise referred to as* ***TREAT****) –* ***MOST RELEVANT TO CCGs***
The majority of risks will be addressed in this way. The purpose of reducing a risk is that whilst continuing with the activity giving rise to the risk, methods or control and assurance are instigated to constrain the risk to an acceptable level.

SHARE
Share is an option that is different in nature from the transfer response. It seeks for multiple parties, typically within a supply chain, to share the risk on a pain/gain share basis. Rarely can risks be entirely shared – the primary risk taker will always need to protect their reputation - but this can be a successful way of encouraging collaboration particularly in programmes and projects.

TRANSFER
For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by requesting assistance or paying a third party to take the risk in another way. Its main use is for financial risk and nearly always involves payment of a premium. The premium cost must be balanced against the benefit of transferring the risk to another party but any financial penalty will be borne by the insurer. It is not possible to transfer reputational risk even if the delivery of a service is contracted out.

STEP 9: IDENTIFY CONTROLS AND ASSURANCES, AND RESULTING GAPS

Once risks are identified then, subject to the degree of risk and its acceptability the following will be identified:

- Controls currently in place and any gaps in those controls (with any necessary actions to close the gaps)
- Assurance in place (both positive and negative) that the risk is currently being managed / controlled to an acceptable level and any gaps in that assurance (with any necessary actions to address the gaps).

A control is a measure in place to mitigate a risk – e.g. an action plan, a policy/procedure or some other aspect of governance such as a committee that has a responsibility or accountability for a risk.

An assurance is evidence that the control is being appropriately discharged, i.e. the action plan is being implemented; a policy/procedure is being appropriately discharged, or copies of minutes for a committee that has accountability for a risk.

Methods of controlling risk must be balanced in order to support advancement and the effective use of resources in order to achieve substantial benefit.

As a general principle, the CCG will seek to control all highly probably risks which have the potential to:

- Cause significant harm to patients, the local community, staff, visitors and any other stakeholders
- Severely compromise the reputation of the CCG
- Result in financial loss that may endanger the viability of the CCG
- Significantly jeopardise the CCG’s ability to carry out its core purpose and/or meet its strategic objectives
- Threaten the CCG’s compliance with law and regulation.

Assurances are obtained from a variety of providers, such as management through their routine checks and reports, internal and external audit and other external assessors such as health & safety Inspectorates, regulators, professional advisors i.e. insurers etc.

The type of assurance provision will be dependent on the level and reliability of assurance required. A greater level of assurance will be provided by an independent source.

The Table below refers to the differing levels of assurance.

Table 6: Levels of assurance

Level	Details
Significant	Taking account of the issues identified, the Governing Body can take significant assurance that the responses upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.
Adequate / Reasonable	Taking account of the issues identified, the Governing Body can take reasonable assurance that the responses upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective. However further action could be taken to improve the effectiveness and efficiency of responses.
Limited / Partial	Taking account of the issues identified, whilst the Governing Body can take some assurance that the responses upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective, action needs to be taken to ensure this risk is managed.
None	Taking account of the issues identified, the Governing Body cannot take assurance that the responses upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective. Action needs to be taken to ensure this risk is managed.

Gaps in control and assurance

Gaps are identified where key controls and assurances are insufficient to reduce the risk of non-delivery of objectives.

A gap in control is deemed to exist where responses are not in place, or where collectively they are not effective and/or, the responses are non-existent or limited. This will be determined through the assurance provided.

A gap in assurance is deemed to exist where there is a failure to gain evidence that the responses are either in place or the response has not been subject to any assurance review.

Wherever gaps in control or assurance are identified, then an action must be defined and allocated to appropriate responsible persons.

However, in all cases an assessment will need to be made as to the level of risk to which the CCG will be exposed as a result of the control failure or assurance gap. This will be achieved through application of the 5x5 risk scoring matrix.

This will ensure:

- consistency in measuring the risk exposure that is deemed to exist; and
- The action can be appropriately prioritised, given that resources are finite and that the action should be proportionate to the risk.

Risk Owners should consider whether the implementation of identified actions (either from Risk Owner identification of control weakness, internal audit reviews of other assurance/inspection programmes) will further reduce the risk exposure proportionate to the resources required and the nature of the risk. Those that Risk Owners consider require implementation should be recorded against the risk in which the control or assurance gap was identified.

Controls and assurance in place should be assessed for their effectiveness to determine whether any gaps exist. The frequency of when these controls are formally assessed as will be determined by the baseline and current risk classification that has been attributed to the risk that they mitigate, or at least when the Risk Register to which they relate is reviewed either by a Risk Owner or a committee to which the project/team that has identified the risk is ultimately accountable.

It is the baseline and current risk classification that will determine the quality, level and priority of assurance work required i.e. a basis for the development of a risk based internal audit plan (see also step 6).

The type and frequency of assurance provision should be obtained within the same timescale as the risk proximity previously identified.

Controls, assurance and gaps in both of these will be included in the documentation used for the Governing Body Assurance Framework and Corporate Risk Register.

STEP 10: DETERMINE ACTIONS – to mitigate gaps in controls and assurances, and to mitigate the risk itself. An indication may also be given on what score is expected once all actions are delivered.

Actions will be dependent on whether they mitigate gaps in controls or assurance, or to mitigate the risk itself. **The timescale applied to actions will also reflect the proximity of the risk identified previously.** Here is worked example.

A provider’s number of cases of C Diff is above target/trajectory, with risk that it will continue to be above target by end of year if not mitigated.

- Control – a provider action plan to mitigate risk and manage down incidence
- Assurance – a monthly/quarterly report on implementation of action plan through CQRM
- Action (to address control) – provider to develop the provider action plan
- Action (to address assurance) – the provider to update CCG on progress through monthly/quarterly CQRM report.
- Gap in control and gap in assurance – if provider does not develop action plan and doesn’t tell CCG that it hasn’t done so
- Gap in control but no gap in assurance – if provider does not develop action plan but it telling the CCG that t hasn’t done so
- Gap in assurance but no gap in control – if provider develops plan but doesn’t keep CCG informed of progress.

- An action would need to happen for a control to be in place – it can’t happen by itself. A control exists, whereas an action does not. An action may have to be implemented in order for a control (or also an assurance) to exist.

One or more actions may also be required to mitigate the risk itself. Actions are not currently separated to distinguish between those which mitigate gaps in control and those which mitigate gaps in assurance. There is only one box available, and therefore risk owners/delegated risk owners need to consider both. "Project Likelihood and Consequence after Mitigation" is the same as the current score.

STEP 11: ESCALATING RISKS

It is recognised that risks occur at different levels across the organisation, with risk impact most likely to be assessed differently at each level. For example, a risk costing 10K more in a 100K project might be considered high, but potentially immaterial at corporate risk level.

Any project or team risk must be re-assessed before it is escalated to appear on the Corporate Risk Register (or GBAF) as a Corporate Risk. A corporate risk is a high level strategic or operational risk graded/scored at 12 and above and identified as affecting strategic aims/goals.

Any project/team risks identified, assessed and aligned to a Risk Register as ‘Extreme’ (i.e. Red rated with a grading score of 12-25 post mitigation) must be re-assessed. Risks to consider for escalation are those where the risk:

a) cannot be managed or mitigated within the project/team;
b) directly impacts on the delivery of a strategic aim/goal;
c) Is not within the project/team remit to rectify.

Any risk re-assessed and remaining at a grade/score of 12 or above would be escalated and appear on the Corporate Risk Register.

Summary of Proposed steps – re-assessment of risks for escalation to the Corporate Risk Register.

STEP 1: Board/Group/Partnership/Forum/Committee/Individual receives a monthly risk report containing the following:

1. Open risks for all its projects with project risk grades/scores and any associated corporate risk scores if (including those escalated to the Corporate Risk Register).

↓

STEP 2: Board/Group/Partnership/Forum/Committee re-assesses each new project risk of 12-25 at corporate risk level using the 5x5 matrix contained within the risk management process flowchart and guidance. A Corporate Risk Owner will also need to be identified (see notes below)

↓

STEP 3: Following re-assessment, there are two options to escalate risks to the Corporate Risk Register (CRR), which would in turn be reported to the Executive Committee (or the Primary Care Commissioning Committee for those which relate to Primary Care):

a) Escalate the risk depending on its materiality (e.g. financial or clinical implications to the operation or reputation of the CCG).
b) Amalgamate existing or new project level risks which combined are a cause for concern to create a new risk for the Corporate Risk Register, which is then graded

↓

STEP 4: Any risks that remain at a score of 12 or above at corporate risk level will be included on the Corporate Risk Register (CRR) and reviewed by the Executive Committee (or the Primary Care Commissioning Committee for those which relate to Primary Care). Any at 15 and above will be automatically escalated to the Governing Body Assurance Framework (GBAF).

Supporting notes on risk escalation

- A Risk Owner, Delegated Risk Owner and Corporate Risk Owner should not be the same person.
- Only the Project Management Office should add the identity of the Corporate Risk Owner to the record on Verto (in the “Risk Owner” box) – so the PMO will need to be informed of the details. Any risk report will show either the project risk owner or corporate risk owner name in the “Risk Owner” box.
- A Risk Owner at project or team level would not be expected to undertake any re-assessment to agree a corporate risk grade/score. Where a project or team risk is not aligned to a Board/Group/Partnership/Forum, the same process applies, however the relevant committee of the Governing Body to which the project/team is ultimately accountable will take the role of the Board/Group/Partnership/Forum in re-assessing project/team risks at corporate risk level.
- Risks identified at project level and subsequently escalated must also remain on the relevant project risk register. The original project risk will remain its original grade/scores on its source register.
- When a risk is re-assesses at corporate risk level, the likelihood of a risk materialising will probably remain the same, whereas the risk impact is more likely to decrease.
- Risks can also be de-escalated back to project/team level through reducing the corporate risk grade/score below the threshold of 12. This de-escalation can be agreed by the Executive Committee. De-escalation from the GBAF is agreed by the Governing Body.
- It is likely that when escalated corporate risks based on an amalgamation of project/team level risks are closed, the individual original project level risks still be open.
- To ensure consistency in application of risk categories, risk registers may be subject to comparison and cross reference before, during and after escalation and de-escalation of risks from the corporate risk register.

Corporate Risk Owner	The individual who is responsible for the management and control of a risk which has been escalated by a Board/Group/Partnership/Forum or individual to the Corporate Risk Register (CRR). The Corporate Risk Owner should always be: (1) A Clinical Commissioning Director (2) A Clinical Lead (3) A Senior manager that is a member of the Governing Body and/or Executive Committee. This individual is responsible for owning the risk (at corporate level) and providing assurance when it is discussed by the Executive Committee or Governing Body. This definition applies to risks on registers presented to the Governing Body (Assurance Framework) and Executive Committee (Corporate Risk Register).

Worked example

1. A project risk with a grade/score of 15 (5 Risk Impact x 3 Likelihood of materialising.
2. Re-assessed by a Board/Group/Partnership/Forum and re-scored at Corporate Level as 9 (3 Risk Impact x 3 Likelihood of materialising).

This risk appears on Corporate Risk Register (CRR) reported to the Executive Committee that same month and will also appear on other Risk Reports. It can be re-assessed and graded/scored by a Board/Group/Partnership/Forum or individual Risk Owner at any time to come further above the threshold grade/score of 12, or to fall below it.

Other principles:

1. Programme Risks can comprise one or more project risks
2. Programme Risks can be identified and escalated in isolation of project risks
3. BUT on Verto, for non-project related risks the “project” scores” are “programme” scores because of the standard field which can’t be changed.

How does Verto show who the Corporate Risk Owner when a risk has been escalated and re-assessed at 12 and above and therefore escalated to the Corporate Risk Register?

Only the Project Management Office should add the identity of the Corporate Risk Owner to the record on Verto (in the “Risk Owner”) – so the PMO will need to be informed of the details. A Risk Owner, Delegated Risk Owner and Corporate Risk Owner should not be the same person. Users should refer to the definitions.

STEP 12: DETERMINE ACCEPTABILITY – or “appetite” (i.e. “Acceptable Score”)

Risk Acceptability /Appetite (i.e. Acceptable Score)

This is the level of risk that is prepared to be accepted or to be exposed to in relation to the risk, post mitigation. Measuring risk acceptability/appetite ensures that risks are considered in terms of both opportunities and threats and are not confined to the financial consequences of a risk materialising. Risks also impact on the capability of the organisation, its performance and its reputation.

Some risks must be taken to achieve strategic aims and goals, but they must be taken in a controlled manner that will reduce the CCG’s exposure to a level deemed acceptable by the CCG Governing Body, relevant auditors and regulators.

Risk appetite is influenced by the individual programmes of work and the NHS landscape. It is recognised that it is not always possible or desirable to eliminate all risks and that systems of control should not be so rigid as to stifle innovation and imaginative use of limited resources in order to achieve health benefits for local residents.

Please note: on Verto there is no separate box for this. Therefore Risk Owners, Delegated Risk Owners and Corporate Risk Owners should have an awareness of what level of risk is acceptable to them – and when they reach that score the risk no longer exists because it has been mitigated down to that score. Following any escalation to the Corporate Risk Register, The Executive Committee will agree what is acceptable.

STEP 13: MONITORING, REVIEWING AND CLOSING RISKS

Implementation of controls, assurances and actions to mitigate risk must be kept under review. Where implementation of action plans is not producing the anticipated results, the risk should be re-assessed and a revised action plan agreed as necessary.

Once all possible actions have been completed or the event has passed, the risk should be recommended to a committee for closure.

Once agreed for closure, the risk is closed and updated as closed on Verto for audit purposes and archived. Risks can be re-opened on Verto as deemed necessary by Risk Owners and/or Corporate Risk Owners.

Who can close risks?

- Open/close/re-open/escalate project level risks – project SRO/ Board/Group/Partnership/Forum

- Open/close/re-open/escalate all corporate risks – Board/Group/Partnership/Forum/ or CCG Executive Committee.

- De-escalate corporate risks only – Governing Body