NHS
Kernow
Clinical Commissioning Group

Risk management strategy and policy

Date approved: 10 April 2021

Document control

Title of document: Risk management strategy and policy
Originating directorate: Head of corporate governance
Originating team: Corporate governance
Document type: Strategy
Subject category: Corporate governance
Author(s) name: Jessica James
Date ratified: 10 April 2021
Ratified by: Executive directors
Review frequency: Every 3 years
To be reviewed by date: 10 April 2024
Target audience: All staff
Can this policy be released under FOI? Yes
Give reasons for exemption if no:

Version control

Version number	Revision date	Revision by	Nature of revisions
V1.0	January 2021	Corporate governance officer	Re-formatting and minor amendments to reflect current roles, responsibilities and structures, move to a 3-year review period and recognition of integrated care systems.

Contents

Introduction

Risk management is the process of identifying, assessing and managing all risks. All organisations work with varying risks daily, some of these are easily managed, others require longer term or more strategic action. A consistent approach to risks is critical in ensuring they are managed appropriately.

NHS Kernow Clinical Commissioning Group (NHS Kernow) is committed to the principles of effective risk management to avoid or limit unnecessary risks to patients, staff, contractors, the public, other stakeholders, the organisations finances, assets, organisational objectives and reputation.

The governing body, its subcommittees and the staff of NHS Kernow will maintain and support the risk management system and ensure that effective mechanisms are in place to reduce the level of risk to the organisation's activities.

NHS Kernow's committee structure can be found in the governance handbook on our website. Should changes to committees be required, including those related to system-wide transformation, the principles, processes and ethos behind NHS Kernow's risk management strategy and policy are expected to continue until such time as the governing body formally agrees any amendments.

This document forms part of the internal control and corporate governance arrangements for NHS Kernow. It provides guidance on the policy, process and procedures for risk management in NHS Kernow.

Policy purpose

This document aims to:

- describe the importance of risk management to NHS Kernow
- support staff to understand their roles in relation to risk management
- ensure a consistent approach to risk management across NHS Kernow

This document:

- sets out the risk management framework which provides assurance to the governing body that robust and effective processes are in place to manage corporate and operational risks
- recommends procedures for the effective identification, prioritisation, treatment and management of risks
- identifies risk management resources
- establishes risk management as an integral part of NHS Kernow culture
- sets out responsibilities for corporate and operational risk for the governing body, committees and staff across NHS Kernow

- describes the standard process to assist staff to identify, analyse and manage risks

Scope and audience

This document applies to all risks that NHS Kernow could be exposed to such as corporate, operational, financial recovery plan, information governance, programme and clinical risks.

At this point in time this document relates to NHS Kernow's own organisational risks. With changes to governance that will be required with change to system working implied by the move to integrated care systems, this policy may need to be updated to accommodate any agreements between the provider and commissioning organisations within Cornwall and the Isles of Scilly as a new way of working develops.

Distribution plan

This document will be made available to all staff, stakeholders and members of the public via the internet document library. Notification of this document will be included in staff update emails. Any significant changes to the document will require approval by the governing body, and it is expected this will take place during a meeting held in public.

Training and support

Ongoing training and support to support the risk management policy and procedures will include regular:

- bespoke risk management training, tailored to staff needs, including sessions for governing body members and executive as required
- guidance and support available on the staff zone risk management page and by contacting the risk management team
- annual mandatory information governance training (compliance monitored through information governance subcommittee and set out in the information governance framework)
- mandatory training, at induction, on health and safety which includes the basics of risk assessment

Roles and responsibilities

Section 5 and appendix 2 set out the specifics of governance and escalation routes for risk through NHS Kernow management and committee structures, including the roles of governing body and constitutional committees.

Appendix 3 sets out the specific roles of various postholders with specific responsibilities, such as senior information risk owner and Caldicott Guardian.

Key risk management roles

See also appendix 3. It is the responsibility of all staff to maintain risk awareness, identify and report risks as appropriate to their line manager and/or director and to cooperate with the organisation in ensuring risk is managed effectively.

It is the responsibility of all managers to ensure risks are assessed, reported and adequately managed. Managers are also expected to communicate risks to their staff, support them to attend any relevant training and to assist any of their staff who may need additional support undertake their responsibilities as outlined above.

The head of corporate governance has day to day responsibility for risk management as part of the corporate governance team and supports all staff and directors in the identification, assessment and reporting or risks. The postholder supports the governing body and committees by providing assurance on the implementation of the risk management policy, the management of the corporate risk register and the review of operational risks.

Accountable director: all risks will be owned by a director who will be responsible for oversight of the management of that risk.

Risk owner: all risks will be assigned to a named individual (usually an operational manager within a directorate team), who is responsible for ensuring the risk is managed, including ongoing monitoring, ensuring controls and actions are in place to mitigate the risks and reporting on the risk including providing updates on these on the organisational risk register.

Risk management process

Risk identification and recording

Consideration should be given to what could pose a potential threat (or opportunity) to the achievement of the organisation's objectives, be they corporate or operational.

Risks and issues are often confused. Risks are things that might happen. Issues are unplanned things that have happened (or that are certain to happen) and require management action. Issues can present risks, for example should the consequences of an issue not be appropriately mitigated, or where an issue is recurring (as with persistent non achievement of a target). In these circumstances the issue will be treated as a risk as it will still require mitigating actions.

Once identified a risk should be described clearly to ensure everyone reading the risk understands it. Guidance on the wording of risks is in appendix 1.

Risk register

As a minimum the risk register will contain:

- date risk was added
- risk reference
- risk description
- ratings of likelihood and impact – current
- accountable director
- risk owner
- actions planned
- dates for actions to be completed
- date risk has been reviewed or is due for review
- tracking of movements in score for example from initial assessment to current
- target scoring on high scoring risks

Guidance on completing a risk register can be found in appendix 1.

Risk assessment and scoring

Risks are scored to ensure a consistent and prioritised approach to their management. This guides operational and planning and resource allocation.

Risks are first assessed on the likelihood of the risk happening and then on the impact (what could happen should the risk occur).

The adequacy and effectiveness of the existing controls, such as systems, policies, training and current practice, should be considered when assessing the likelihood.

Impacts should be assessed based on what the impact of the risk would be in most circumstances within the current environment and what is reasonably foreseeable, rather than the worst-case scenario.

The risk score is based on the combination of the likelihood and impact scores. Appendix 4 sets out the scoring tables based on a scale of 1 to 5 and the matrix which is used to ascertain the risk score and red-amber-green (RAG) status.

Risk scoring is subject to moderation and oversight through several mechanisms:

- accountable directors review the assessments and scoring on each risk within their responsibility as part of the regular review cycle
- risk reports are sent to the joint senior leadership team (JSLT) meeting (or its equivalent) at least 3 times a year
- committees receive their red corporate risks and any other risks escalated for their attention and their review incudes consideration of the appropriateness and accuracy of scoring
- the corporate governance team provide feedback, where appropriate, on risk scoring

Action planning

Once a risk has been assessed, consideration should be given to whether further management action is required to either eliminate the risk, seek to minimise the likelihood and/or impact or maximise the likelihood of opportunities. It is not always possible to identify and fully implement actions to eliminate or minimise a risk. Where this is the case, the significance of the remaining risk must be understood and NHS Kernow should confirm that it is prepared to accept that level of risk. The reporting and oversight of risks section and appendix 2 provide guidance on who can accept risks.

Monitoring and closure

The implementation of actions and the level of risk should be kept under review. If actions are being implemented but the risk is not reducing as anticipated, the risks should be reassessed and revised action plan agreed.

Where all possible or reasonable actions have been completed, but some risk remains (albeit at a reduced impact or likelihood) a risk should be accepted. This means no additional mitigating actions are required. NHS Kernow will automatically accept all risks scoring less than 4 (green risks). The accepted risk will be reviewed periodically by the accountable director to ensure circumstances have not changed. Acceptance of risks must be carried out in accordance with the risk management governance set out in the reporting and oversight of risks section and appendix 2 .

If a risk has crystallised and/or an event has happened or passed, the risk should be closed and removed from the register. Closing of risks must be carried out in accordance with the risk management governance set out in the reporting and oversight of risks section and appendix 2.

Reporting and oversight of risks

Appendix 2 provides details on the risk roles for each key committee, for example the governing body. This includes their roles in reviewing, adding, removing, accepting, escalating and de-escalating risks and scrutinising the mitigation and scoring of risks, and what type and level of risks they hold these responsibilities for. It also provides information on the frequency and content of reporting to these groups. NHS Kernow has an IT system, called information reporting and intelligence system (IRIS), which is used to facilitate the reporting on risks and the assurance framework. Any significant changes to the responsibilities and reporting will be agreed in advance with governing body and the key committees.

Risk appetite and tolerance

A risk appetite statement involves an organisation defining the level of risk it is willing to accept before activity is deemed necessary to reduce it. This allows the organisation to focus its management efforts. NHS Kernow will review its risk appetite in advance of each financial year.

Appendix 5 provides further details on the risk appetite of NHS Kernow.

NHS Kernow recognises that it may sometimes need to tolerate a higher level of risk for example whilst pursuing innovation and challenging current practice to reduce future risk or to avoid compromising quality of care.

NHS Kernow's current risk tolerance for corporate risks, in line with the general appetite statement above, is described below:

Risk Score	Tolerance	Actions
Less than 4	High	• Risk accepted, 6 monthly review. • Report to relevant interest forums (for example information governance risks to the information governance sub-committee).
4 to 10	Moderate	• Quarterly review. • Reporting as above. • Acceptance or removal requires committee approval.
12	Low	• Monthly review. • Report to committees at least 3 times a year. • Reviewed by JSLT if escalated. • Acceptance or removal requires committee approval.
15 or more	Very low	• Add to assurance framework. • Monthly review. • Reviewed by JSLT at least 3 times a year. • Report to committees at each meeting. • Report to governing body at least 3 times a year. • Acceptance or removal requires governing body approval.

Governing body assurance framework

The governing body is responsible for ensuring the delivery of the strategic objectives of NHS Kernow. The governing body assurance framework sets out the key risks to delivery of these objectives (principal risks) and the systems, processes and structures (controls) that are in place to manage them. It then identifies any gaps in those controls and sources of assurance that the organisation can access to enable them to assess whether they are successfully managing the principal risk and achieving the objective.

The assurance framework is seen by the governing body at least 3 times a year. The audit committee maintains oversight of the assurance framework and its management as part of its remit to review systems of integrated governance, risk management and internal control across NHS Kernow.

Principal risks on the assurance framework include information on the adequacy of the key controls identified and the adequacy of the assurance expected or received. This provides additional information to the governing body on the sufficiency and effectiveness of the systems in place and planned to mitigate risk to strategic objectives. Detail on the scoring of adequacy is in appendix 1.

Risk management in partnership

NHS Kernow is committed to working in partnership with the people of Cornwall and the Isles of Scilly. NHS Kernow routinely consults and engages widely with the public regarding the services we commission, allowing the public to be aware of and engaged in managing the risks that impact upon them.

The governing body will continue to receive, at least 3 times a year, risk and assurance framework reports and these will continue to be part of the agenda for the governing body held in public. By exception, risks will be reported in the private session of the governing body, where circumstances require it.

Throughout the year, the head of corporate governance will continue to liaise with risk leads from key providers to ensure that where appropriate, corporate red risks and assurance framework entries are reflected across organisational boundaries.

Changes to this approach are anticipated in due course with the development of strategic commissioning and integrated care systems. These changes will be reflected as necessary in policy documents.

Managing risk of fraud and bribery

Fraud

NHS Kernow's accountable officer and chief finance officer have a responsibility to ensure that the organisation has adequate counter fraud measures in place to manage the risk of fraud in accordance with NHS protect counter fraud strategy.

The government functional standard 013 counter fraud applies to all NHS organisations from 1 April 2021. This standard requires the CCG to carry out a comprehensive local risk assessment on an annual basis to identify fraud, bribery and corruption risks, and have a counter fraud provision that is proportionate to the level of risk identified.

Risk analysis is undertaken in line with government counter fraud profession fraud risk assessment methodology. It is recorded and managed in line with this risk management policy and included on the appropriate risk registers. Measures to mitigate identified risks, such as specific proactive reviews, are included in the annual counter fraud work-plan and progress is regularly reported to the audit committee.

The local counter fraud specialist (LCFS) will inform NHS Kernow of potential fraud risks so they can be effectively assessed. Where risks are identified these will be included on the NHS Kernow risk register so they can be proactively addressed. Similarly, all fraud risks identified by the organisation will be communicated to the LCFS.

The audit committee and the chief finance officer are kept abreast of any issues relating to fraud throughout the year.

In addition, NHS Kernow will participate in national and local pro-active exercises throughout the year, designed to identify fraud and reduce the likelihood of specific fraud risks to which it may be vulnerable.

Bribery

The Bribery Act 2010 introduced a corporate offence of failure to prevent bribery by persons working on behalf of a business. However, for NHS Kernow to have a statutory defence to the corporate offence, it must demonstrate that the 6 adequate procedures have been considered, assessed, and where appropriate, measures taken.

The 6 adequate procedures are as follows:

1. Proportionate procedures to prevent bribery.
2. Top level commitment.
3. Risk assessment.
4. Due diligence.
5. Communication (including training).
6. Monitoring and review.

NHS Kernow will assess the nature and extent of its exposure to potential external and internal risks of bribery on its behalf by persons associated with it. The organisation will ensure that its risk assessment procedures accurately identify and prioritise the risks it faces, whatever its activities, customers or sector.

The risk assessment will encompass the following characteristics:

- oversight of the risk assessment by top level management
- appropriate resourcing reflecting the scale of NHS Kernow's business and the need to identify and prioritise all relevant risks
- identification of the internal and external information sources that will enable risk to be assessed and reviewed
- due diligence of associated persons (should be proportionate to the identified risk)
- accurate and appropriate documentation of the risk assessment and its conclusions

More information can be found in our anti-fraud and bribery policy.

Information security risk assessment and management

To ensure effective implementation of information risk processes, there should be a comprehensively scoped and formally documented plan and programme. This should consider security risks to information assets in NHS Kernow, including systems and media used in processing or storing that information and online and internet facing services. Consideration of the potential impacts on business continuity and protection of personal and corporate data will be key to this plan and programme.

A formal information security risk assessment and management method should be implemented for all information assets, to ensure threats, vulnerabilities and impacts are assessed, included in the organisations risk register and acknowledged in our information governance assurance framework. In undertaking these risk assessments available methodologies and supporting products will be considered. This may include the information security forum's information risk assessment (IRAM) and the International Organisation for Standardisation's (ISO) 27005:2010, information security risk management.

Each risk assessment will be clearly scoped, systematic and seek to identify, quantify and prioritise the information risks to NHS Kernow's business functions. Consideration will also be given to information risks which may impact on our partners. Where appropriate controls will be put in place and their effectiveness monitored. This monitoring will be informed by information on incidents and system log files. Periodic update reviews of existing risk assessments will be undertaken to consider possible changes.

To assess risks relating to information governance and cyber related risks, each information asset owner will complete a risk assessment using the CCG adapted information security management system (ISMS) risk assessment tool.

Monitoring and review of risk management in NHS Kernow

The risk management strategy and policy will be reviewed every 3 years. Significant changes will require approval by the governing body, while minor amendments may be agreed in line with the NHS Kernow policy on the development and ratification of policies and similar documentation. This 3 yearly review schedule will not prevent ad hoc review as necessary in line with procedural, legislative or best practice changes.

The risk register and assurance framework are live documents and reviewed regularly throughout the year, with reports to audit committee to provide assurance on the effectiveness of the risk management procedures in NHS Kernow.

Risk and assurance management is subject to regular (annual) review by internal audit with reports to audit committee.

NHS Kernow will produce an annual governance statement, as required by NHS England and improvement to provide assurance on the stewardship of the organisation.

The governance statement, corporate risk register and governing body assurance framework are intended to provide assurance that risk management strategy is being complied with. If appropriate, they will reference any recommendations for improvement.

The annual governance statement is reviewed and approved annually by the audit committee then submitted to governing body as part of the annual report and accounts.

Appendix 1: Glossary and guidance on risk register completion

Accepting a risk
Means, essentially, agreeing to live with the risk as it stands. The problem remains, but no further action is intended to reduce it. Accepted risks should be reviewed periodically to ensure circumstances have not changed. Acceptance of risks requires agreement, see risk management process.

Actions
Are the smaller steps towards risk reduction such as developing a service specification or discussion at contract meetings and should be updated by the risk owner or director. Dates given on actions are expected dates of delivery. Updates should indicate when they have been achieved or slipped or missed.

Adequacy of controls (assurance framework)
Seeks to indicate whether key identified controls are in place and robust, or whether there are gaps. This is assessed by corporate governance and the senior lead and director responsible for the principal risk. Controls are shown as either in place, partially in place or not in place.

Adequacy of assurance or validation score (assurance framework)
Seeks to indicate the value and strength of assurance and is usually completed by the corporate governance team.

Description	Examples
Weak assurance	Source is based on assumption rather than data (“we think it’s ok”).
Moderate assurance	Indirect, not validated or internal only. For example, self-assessments. Sickness rates as an indicator of staff morale. Dated assurance may also be here, for example last year’s survey.
Strong assurance	Recent, relevant and robust assurance. External or third party assurance, which is direct and sufficient. For example, national performance data, audit reports.

Assurance framework
Document that provides a structure and process for the governing body to focus on key risks which could prevent achievement of strategic objectives, ensuring there are effective controls in place to avoid those risks materialising and providing assurance on the effectiveness of those controls.

Assurance
Provides information on the effectiveness of controls in place. It can provide confidence they are working or highlight where additional action is required. In risk reporting, the

status is based on the RAG ratings, for example in performance reports or provided by internal audit, and the date refers to when the assurance was received. This field should be completed by the senior or executive lead for the principal risk, or by the corporate governance team.

Control
Something that has been put in place to prevent the risk or reduce the harm for example a policy, a safe system of work, monitoring processes, education and training.

Corporate risk
A risk where the impact and/or the actions required are at an organisational level.

Milestones
The big steps towards risk reduction, such as delivery of all actions on a plan, achievement of milestones on a trajectory or commencing procurement. These should be updated by the risk owner or director. Dates given for milestones are expected dates of delivery. Updates should indicate when they have been achieved or slipped or missed.

Operational risk
A risk where the impact and/or the actions required are at a departmental level.

Principal risk
A risk to delivery of a strategic objective, identified on the governing body assurance framework.

Proximity
This is a measure of when the risk could occur, particularly relevant for time-bound risks on programmes and projects.

Risk appetite
The organisation's agreed level of acceptance for risks, outlining at what stage activity is necessary to mitigate a risk. See section 6 and appendix 5.

Risk assessment
The process of establishing the likelihood and consequence of a risk and giving this a risk rating (see appendix 4 for detail).

Risk description
Risks should include references to the cause, event and effect. For example, "There is a risk X (the cause) happens leading to Y (the event) and resulting in Z (the effect)". A real example might be "there is a risk difficulty recruiting to vacancies in the complaints team leads to delayed responses to enquiries resulting in poor patient experience and harm to reputation."

Risk management

The process of identifying, assessing and managing all potential threats and opportunities that could have an impact on the delivery of the organisation's objectives and business.

Risk register
Document or database which contains details of risks identified across the whole organisation. These can be at any rating.

Risk
An uncertain event or set of events that should it occur will have an adverse effect on the objectives of the organisation.

Risk tolerance
The level of risk an organisation is willing to tolerate before it needs to take additional action or review. NHS Kernow will tolerate low scoring risks by letting them sit with directors but, as they get to high amber or red, they will receive focus at committees and governing body.

Strategic objectives
High level strategic targets agreed by the governing body.

Target scoring
This is the level of risk score the risk is expected to be reduced to by a particular date, often the end of a financial year, by implementation of the existing controls and planned actions.

Appendix 2: Governance

The governing body:

- has responsibility for ensuring appropriate structures are in place to implement effective risk management and appropriate resources are committed to adequately control identified risks
- accepts, formally and publicly, a collective role in providing risk management leadership in the CCG and ensures all decisions reflect this
- receives regular reports on the assurance framework or corporate red risks (usually 3 times a year), containing summary information on new and draft risks, risks closed by committees, risks for closure by the governing body, the risk profile of the organisation, updates missed, increases and decreases in score, target scores, adequacy of controls and assurance and recent key milestone and actions as well as full details on each red corporate risk and assurance framework entry
- retains the responsibility for decisions on the removal or acceptance of red corporate risks
- can add any risks it feels should be on the register, of any type or score

The audit committee:

- reviews the establishment and maintenance of an effective system of risk management across the whole of CCG's activities
- provides assurance to the governing body on the adequacy of its wider organisational controls
- reviews the establishment and maintenance of an effective system of integrated governance, risk management and internal control that supports the achievement of the organisation's objectives
- receives regular reports on the risk register and assurance framework, containing information on the functioning of the risk management and assurance framework process as well as summary information on new and draft risks, risks closed by committees, risks for closure by the governing body, the risk profile of the organisation, updates missed, increases and decreases in score, target scores, adequacy of controls and assurance and recent key milestone and actions
- can add any risks it feels should be on the register, of any type or score
- can suggest the removal or acceptance of any risk, subject to approval as per the risk tolerance table in section 6

The finance and performance committee:

- review the CCG's monthly financial performance and provider performance information and identify key issues and risks requiring discussion or decision by the governing body

- have responsibility to review the financial and performance related risks contained within the corporate risk register
- review their red and high amber corporate risks on a regular basis with reports containing summary information on the number and RAG of risks, new and draft risks, risks for closure by the committee, updates missed, increases and decreases in score, target scores, adequacy of controls and recent key milestone and actions as well as full details on each risk
- can add new risks and close non-red corporate risks
- provide a report, via the chair of the committee, to the governing body after each committee meeting which includes the committee's review of risks where this took place

The quality committee:

- review quality information, identifying key issues and risks requiring discussion or decision by the governing body
- give an opinion on the stewardship of commissioned services and its ongoing concern status
- provide the governing body with assurance that commissioning risks are being effectively managed and mitigations are in place seeking their support and involvement, where necessary
- have responsibility to review the quality related risks contained within the corporate risk register
- review their red and high amber corporate risks on a regular basis, with reports containing summary information on the number and RAG of risks, new and draft risks, risks for closure by the committee, updates missed, increases and decreases in score, target scores, adequacy of controls and recent key milestone and actions as well as full details on each risk
- can add new risks and close non-red corporate risks
- provide a report, via the chair of the committee, to the governing body after each committee meeting which includes the committee's review of risks where this took place

The people and organisational governance committee:

- review HR and other essential information pertaining to its terms of reference, identifying key issues and risks requiring discussion or decision by the governing body
- have responsibility to review the workforce and organisational governance related risks contained within the corporate risk register
- review their red and high amber corporate risks on a regular, usually bi-monthly, basis, with reports containing summary information on the number and RAG of risks, new and draft risks, risks for closure by the committee, updates missed, increases and decreases in score, target scores, adequacy of controls and recent key milestone and actions as well as full details on each risk

- can add new risks and close non-red corporate risks
- provide a report, via the chair of the committee, to the governing body after each committee meeting which includes the committee's review of risks where this took place

The primary care commissioning committee:

- review essential information pertaining to its terms of reference, identifying key issues and risks requiring discussion or decision by the governing body
- have responsibility to review the primary care commissioning related risks contained within the corporate risk register
- review their red and high amber corporate risks on a regular basis, with reports containing summary information on the number and RAG of risks, new and draft risks, risks for closure by the committee, updates missed, increases and decreases in score, target scores, adequacy of controls and recent key milestone and actions as well as full details on each risk
- can add new risks and close non-red corporate risks
- provide a report, via the chair of the committee, to the governing body after each committee meeting which includes the committee's review of risks where this took place

The joint senior leadership team (or equivalent):

- receive a report at least 3 times a year on corporate risks containing detail on all red corporate risks and any high amber risks escalated by a committee for their attention
- take an overview of risks across the whole organisation, allowing consideration of the appropriateness of risk scoring and any gaps in the register
- can add any risks it feels should be on the register, of any type or score
- can suggest the removal or acceptance of any risk, subject to approval as per the risk tolerance table in section 6

Accountable directors:

- can access their risks at any time using the IRIS system
- receive prompts to review their risks monthly to provide scrutiny on scoring, assurance, actions and milestones, accuracy and gaps in the register
- can add any risks they feel should be on the register, of any type or score
- can suggest the removal or acceptance of any corporate risk, subject to approval as per the risk tolerance table in section 6
- can remove or accept any operational risk within their remit

Other committees or boards:

- regularly review relevant risks
- escalate to directors where appropriate

- can raise new risks for director approval
- can suggest the removal or acceptance of any risk for appropriate approval

Appendix 3: Roles and responsibilities

The chief officer is the accountable officer, with responsibility for implementing working arrangements which secure effective and appropriate risk management within NHS Kernow. The chief officer has designated the director of people and corporate services as the director with responsibility for risk.

The deputy director of corporate governance is responsible for ensuring effective corporate assurance, governance and risk procedures are in place across the organisation.

The chief finance officer is responsible for arrangements to review, evaluate and report on financial control and regular assessment of and reporting on financial risks and the financial aspects of other organisational risks. The post holder also acts as the governing body lead for counter fraud and information governance

The chief nursing officer is responsible for ensuring robust systems are in place for quality governance to assure and improve quality of care for all patients, taking the lead on risks relating to the clinical quality and safety of services and ensuring the quality aspects of other organisational risks are apparent and addressed.

The Caldicott Guardian is a strategic, advisory and facilitative role with the aim that the practice of NHS Kernow and its employees will comply with high practical standards for handling patient information. The chief nursing officer holds the role of Caldicott Guardian for NHS Kernow.

The senior information risk officer (SIRO) provides focus for the management of information risk at governing body level. The chief finance officer holds this role.

The head of corporate governance provides a formal lead on corporate risk management across the organisation and is responsible for ensuring implementation of the corporate risk register and assurance framework and reporting on this.

The corporate governance team provide NHS Kernow with advice and support on security and health and safety and are responsible for identifying risks arising from claims as they progress and ensuring that these are brought to the attention of the head of corporate governance.

The head of information governance provides advice and support on issues and risk arising from the management of information.

The complaints manager is responsible for identifying risks arising from complaints and ensuring these are brought to the attention of the head of corporate governance.

The local counter fraud specialist (LCFS) provides staff with advice and support in accordance with the NHS counter fraud authority strategy and carries out national and

local work to raise awareness and reduce the likelihood and impact of fraud. They investigate suspected cases of fraud and corruption in accordance with NHS counter fraud authority guidance. Where system weaknesses are identified these will be reported to NHS Kernow, internal and external audit as appropriate.

NHS Kernow also has a security management service provided by TIAA.

Appendix 4: Impact and likelihood scoring

Table 1 risk impact score: choose the most appropriate domain for the risk from the left-hand side of the table, then work along the columns to assess the severity on a scale of 1 to 5. Note: the exact impact may not be included below, therefore please use examples given as indicative.

Impact type: Safety, quality and operational

Score 1 – Very low	Score 2 – Low	Score 3 – Moderate	Score 4 – High	Score 5 – Very high
• Minor reduction in quality of treatment or service. • No or minimal effect on patients or staff. • Short term low staffing with temporary reduction in service (1 day). • No time off work. • No or minimal treatment required.	• Single failure to meet national standards of quality of treatment or service. • Low effect for small number of patients or staff if unresolved. • Up to 3 days off work. • Minor injuries or illness.	• Repeated failure to meet national quality standards. • Moderate effect for multiple patients or staff if unresolved. • 3 to 14 days off work or RIDDOR reportable. • Moderate injury or illness requiring professional intervention.	• Ongoing non-compliance with national standards for quality of treatment or service. • Significant effect for numerous patients or staff if unresolved. • 14+ days off work. Major injury or long-term incapacity.	• Gross failure to meet national standards with totally unacceptable levels of quality of treatment or service. • Very significant effect for large number of patients or staff if unresolved. • Irreversible health effects or death.

Impact type: Performance and reputation

Score 1 – Very low	Score 2 – Low	Score 3 – Moderate	Score 4 – High	Score 5 – Very high
• Not relevant to priorities. • No adverse media coverage and/or negative recognition from the public. • No or minimal breach in statutory duty.	• Minor impact on achieving priorities. • Low level of adverse media coverage and/or negative public interest. • Breach of statutory legislation.	• Moderate impact on achieving priorities. • Moderate level of adverse media coverage and/or negative public interest. • Single breach of statutory duty or improvement notice.	• High impact on achieving priorities. • High level of adverse media coverage or negative public interest. • Multiple breaches of statutory duty, enforcement action or improvement notices.	• Priorities will not be achieved. • National adverse media coverage and/or total loss of public confidence. • Multiple breaches or prosecution.

Impact type: Finance

Score 1 – Very low	Score 2 – Low	Score 3 – Moderate	Score 4 – High	Score 5 – Very high
• Loss of up to 1% of budget. • Failure to deliver up to 1% of planned savings.	• Loss of 1% to 5% budget. • Failure to deliver 1% to 5% of planned savings.	• Loss of 5% to 10% budget. • Failure to deliver 5% to 10% of planned savings.	• Loss of 10% to 20% budget. • Failure to deliver 10% to 20% of planned savings.	• Over 20% budget loss. • Failure to deliver 20%+ of planned savings.

Impact type: Scope, capacity and timescales

Score 1 – Very low	Score 2 – Low	Score 3 – Moderate	Score 4 – High	Score 5 – Very high
• Project is slightly out of scope and/or slight schedule slippage. • Short-term low staffing level that temporarily limits project delivery.	• Project out of scope and schedule slippage causing minor delays. • Low staffing level that reduces service quality. • Lack of skills, experience or capacity leading to delay in project delivery.	• Project out of scope with moderate impact on delivery benefits. • Schedule slippage requiring 5-10% more time. • Lack of skills, experience or capacity leading to late delivery of key objective or service.	• Programme is out of scope, but measures are in place to reduce impact on programme outcome. • Uncertain delivery of key objective or service due to lack of skills, experience or capacity.	• Programme is well behind schedule and highly unlikely to realize expected benefits. • Non-delivery of key objectives • Significantly low level of staff skills, experience and/or capacity.

Table 2 Risk likelihood score: what is the likelihood of the consequence occurring?

Score	Descriptor	Description
1	Rare	• Not expected to occur apart from in exceptional circumstances. • Currently well managed or controlled.
2	Unlikely	• Do not expect it to happen or recur but it could. • Satisfactorily managed or controlled.
3	Moderate or possible	• Event might occur at some time. • Some management or control.
4	Likely	• Will probably happen or recur. • Weaker management or control.
5	Almost certain	• Is expected to occur in most circumstances. • No or ineffective management or control.

Table 3 Risk matrix: multiply the impact and likelihood scores to get your overall risk score and colour

Description	Impact score 1: Very low	Impact score 2: Low	Impact score 3: Moderate	Impact score 4: High	Impact score 5: Very high
Likelihood score 1 - rare	1	2	3	4	5
Likelihood score 2 - unlikely	2	4	6	8	10
Likelihood score 3 – moderate or possible	3	6	9	12	15
Likelihood score 4 - likely	4	8	12	16	20
Likelihood score 5 - almost certain	5	10	15	20	25

Appendix 5: NHS Kernow risk appetite

Each principal risk has been considered and a tolerance score agreed. These indicate the level of risk appetite NHS Kernow has.

Improve health and wellbeing and reduce inequalities by working in partnership and creating opportunities for our citizens.

Principal risk	Tolerance score	Risk appetite level
NHS Kernow and system partners do not work together to actively reduce health inequalities in the services we offer.	12	High

Provide safe, high quality, timely and compassionate care and support in local communities wherever possible and informed by people who use services

Principal risk	Tolerance score	Risk appetite level
Partners do not deliver safe and clinically effective care.	12	High
Partners do not deliver safe and clinically effective care.	9	Moderate
Partners are unable to consistently and sustainably deliver timely access to care.	9	Moderate
Partners do not deliver a positive experience of care.	12	High

Working efficiently so health and care funding gives maximum benefits Working efficiently so health and care funding gives maximum benefits

Principal risk	Tolerance score	Risk appetite level
Inability to deliver NHS Kernow's agreed financial plan (which may lead to legal directions).	9	Moderate

Make Cornwall and the Isles of Scilly a great place to work in health and social care

Principal risk	Tolerance score	Risk appetite level
Poor workforce health, staff morale plus inadequate capacity or capability in NHS Kernow will impact our ability to move from good to great.	9	Moderate
The organisation does not comply with core governance or corporate requirements and is unable to provide the appropriate assurances.	4	Low.

Create the underpinning infrastructure and capabilities that are critical to delivering high quality care and support

Principal risk	Tolerance score	Risk appetite level
Inappropriate structures and/or governance arrangements may impact our ability to effectively transform care and harm relationships with system colleagues and other stakeholders.	10	Moderate

Ensure the commissioning of services takes account of COVID19 recovery plans, any subsequent peaks of infection as well as agreed long term plan expectations

Principal risk	Tolerance score	Risk appetite level
NHS Kernow and system partners are unable to optimise resources resulting in constrained capacity services, longer waiting times and continued health and care inequalities.	10	Moderate

Appendix 6: Equality impact assessment

An equality impact assessment is used to establish how a policy or similar document may impact on individuals, communities or equality groups to identify and minimise or remove any disproportionate impact. A full impact assessment should be undertaken for policies, strategies, procedures or projects which are anticipated to have an impact on members of the public. Read guidance on how to complete this document.

Name of policy or service to be assessed: Risk management strategy and policy
Department or section: Corporate governance
Date of assessment: 19 March 2021
Person(s) responsible for the assessment: Head of corporate governance
Is this a new or existing policy? Existing

Aims, objectives and purpose of the policy

Describe the aims, objectives and purpose of the policy:

Provides NHS Kernow's approach to risk and risk management as part of the overall system of internal control.

Who is intended to benefit from this policy, and in what way?

All staff, NHS Kernow itself and the wider community. The strategy is intended to ensure that the CCG can ensure the safe and efficient commissioning of healthcare services to meet identified local needs; to maintain a safe environment for staff, contractors and visitors; to minimise financial loss to the organisation and to demonstrate to the public that NHS Kernow is a safe and efficient organisation.

What outcomes are wanted from this policy?

Effective management of risk across NHS Kernow. NHS Kernow aims to ensure that risks (whether to staff, patients, contractors, visitors, the general public or the organisation itself) are identified, consistently graded, and that reasonably practicable action is taken to reduce or eliminate the chances of such risks occurring. Effective risk management assists in ensuring NHS Kernow is not acting in a discriminatory way.

What factors and forces could contribute or detract from the outcomes?

Lack of a policy and strategy would increase the chances of uncontrolled risk occurring, with potential adverse consequences to staff, patients, the public, contactors and the organisation as above. It would also place the CCG in breach of central requirements.

Who are the main stakeholders in relation to the policy?

NHS Kernow and all its staff.

Who implements the policy, and who is responsible for the policy?

All staff, led by directors and the corporate governance team.

Differential impacts

Perspective of race, nationality and/or ethnic origin

Does this have a positive or negative impact on black, Asian and minority ethnic (BAME)?

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately. Section 4.1 highlights the responsibility of managers to assist their staff in understanding risk management and their role in it.

How will any negative impact be mitigated?

None anticipated.

Perspective of sex

Does this have a positive or negative impact on people who identify as male, female or intersex?

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately.

How will any negative impact be mitigated?

None anticipated.

Perspective of disability

What is the positive or negative differential impact on people from the perspective of disability?

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately. Section 4.1 highlights the responsibility of managers to assist their staff in understanding risk management and their role in it.

How will any negative impact be mitigated?

None anticipated.

Perspective of sexual orientation?

Does this have a positive or negative impact on people who identify as heterosexual, lesbian, gay, bisexual, pansexual or asexual?

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately.
How will any negative impact be mitigated?

None anticipated.

Perspective of age

What is the positive or negative differential impact on people from the perspective of age?

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately.
Section 4.1 highlights the responsibility of managers to assist their staff in understanding risk management and their role in it.

How will any negative impact be mitigated?

None anticipated.

Perspective of religion or belief

What is the positive or negative differential impact on people from the perspective of religion or belief?

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately. Section 4.1 highlights the responsibility of managers to assist their staff in understanding risk management and their role in it.

How will any negative impact be mitigated?

None anticipated.

Perspective of marriage and civil partnership

What is the positive or negative differential impact on people from the perspective of marriage and civil partnership? This is particularly relevant for employment policies.

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately.

How will any negative impact be mitigated?

None anticipated.

Perspective of gender re-assignment

Does this have a positive or negative impact on people who identify as trans or transgender, non-binary or gender fluid?

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately.

How will any negative impact be mitigated?

None anticipated.

Perspective of pregnancy and maternity

Does this have a positive or negative impact on people who are pregnant, breast feeding mothers, or those on maternity leave?

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately.

How will any negative impact be mitigated?

None anticipated.

Other identified groups

Policy assists the organisation in ensuring that risks of differential impacts are managed appropriately. Section 4.1 highlights the responsibility of managers to assist their staff in understanding risk management and their role in it.

How will any negative impact be mitigated?

None anticipated.

Human rights values

How have the core human rights values of fairness, respect, equality, dignity and autonomy been considered in the formulation of this policy, service or strategy?

Section 1 of the strategy states the aim of the document, which demonstrates intention for safety for all stakeholders: "NHS Kernow clinical commissioning group (NHS Kernow) is committed to the principles of effective risk management to avoid or limit unnecessary risks to patients, staff, contractors, the public, other stakeholders, the organisations finances, assets, organisational objectives and reputation."

Promoting risk assessment encourages consideration of individual needs. Good risk management will assist the CCG in identifying and responding to risks of non-compliance with race and human rights legislation and good practice and ensure the relevant controls are in place.

Which of the human rights articles does this document impact?

☒ To life
☐ Not to be tortured or treated in an inhuman or degrading way
☐ To liberty and security
☐ To a fair trial
☐ To respect for home and family life, and correspondence
☐ To freedom of thought, conscience and religion
☐ To freedom of expression
☐ To freedom of assembly and association
☐ To marry and found a family
☐ Not to be discriminated against in relation to the enjoyment of any of the rights contained in the European Convention
☐ To peaceful enjoyment of possessions

What existing evidence (either presumed or otherwise) do you have for this?

Right to life is implicit - policy considers for example safe purchasing of healthcare and provider performance concerns. risk assessment is about reducing and preventing harm.

How will you ensure that those responsible for implementing the policy are aware of the human rights implications and equipped to deal with them?

Staff are required to undertake mandatory training in health and safety which includes risk assessment. They are also required to undertake training on equality and human rights.

Public Services Social Value Act 2020

NHS Kernow is committed and obliged to fulfil the requirements of the Public Services Social Value Act 2012. This Act requires the organisations to consider how services commissioned or procured might improve the economic, social and environmental wellbeing of an area.

Please describe how this will support and contribute to the local system, wider system and community.

This policy does not relate to the commissioning or procuring of services.

Describe how the policy contributes towards eliminating discrimination, harassment and victimisation.

Promoting risk assessment encourages consideration of individual needs. Good risk management will assist the CCG in identifying and responding to risks of non-compliance with race and human rights legislation and good practice and ensure the relevant controls are in place.

Describe how the policy contributes towards advancing equality of opportunity.

As above.

Describe how the policy contributes towards promoting good relations between people with protected characteristics.

As above.

If the differential impacts identified are positive, explain how this policy is legitimate positive action and will improve outcomes, services and/or the working environment for that group of people.

No differential impacts identified.

Explain what amendments have been made to the policy or mitigating actions have been taken, and when they were made.

No amendments made.

If the negative impacts identified have been unable to be mitigated through amendment to the policy or other mitigating actions, explain what your next steps are using the following equality impact assessment action plan.

No negative impacts identified.

Equality impact assessment action plan

Issues to be addressed	Action required	Responsible person	Timescale for completion	Action taken	Comments
N/A	N/A	N/A	N/A	N/A	N/A

Signed (completing officer): Jessica James

Date: 4 March 2021

Signed (head of department or section): Trudy Corsellis

Date: 18 March 2021

Please ensure that a signed copy of this form is sent to both the corporate governance team with the policy and the equality and diversity lead.