Risk Management Procedure		
Standard Operating Procedure (SOP)		
Prepared by:	**Risk Officer**	
Presented to:	**Risk Group**	**Date: 15 December 2022**
Ratified by:	**Risk Group**	**Date:**
		Review date: 15 December 2025
Relating to documents:		Risk Management Strategy Risk Management Policy

Purpose of this document – California Software Company Limited (Calsoft) is required to have an organisation-wide process for the effective identification and maintenance of health and social care risks. This will support the delivery of high quality, safe health and social care for the people who use our services and minimise risks to staff.

This document has been written to act as a procedure to identify, rate and review risks within Calsoft..

Scope of this SOP – This document refers to all employees in our organisation.

Competencies required – No specific competencies are required to follow this procedure however it is recommended that the Risk Management Strategy and Risk Management Policy are read and understood. Risk Assessments are part of the mandatory Health and Safety Training for managers, provided on a three-yearly basis**.**

Responsibilities – All staff have a responsibility to understand risk and to keep up to date with risk management issues. Managers are accountable for taking ownership, recording and reviewing risks on both Risk Assessment Forms and the Datix Risk Management System, depending upon the level of risk to our organisation. They may assign a Risk Handler to assist with this.
Risk Owners / Managers are responsible for implementing and monitoring any identified and appropriate risk management control measures within their designated areas and scope of responsibility. Full responsibilities are detailed within the Risk Management Policy.

1. Risk Management Procedure:

1.1 Risk management is a systematic process, to be effective it needs to be holistically applied strategically and operationally to all systems, processes and services. It should include (but not be limited to) the following factors:

- Clinical Safety, Performance, Environment, Finance, Health and Safety, Infection Control and Prevention, Information and Communication Technologies, Information Governance, Operational Issues, User Experience and Reputational.

1.2 The risk management procedure is based on the following key steps:

- **O**bjectives - establish the context of the risk against one or more of the corporate strategic objectives (what is the cause and effect against these objectives).
- **R**isks - risk identification and assessment (analyse, evaluate and prioritise).
- **C**ontrols - what controls are already in place or can be introduced with immediate effect to reduce the likelihood of this risk happening (including actions for future controls).
- **A**ssurance - monitoring and reviewing of the situation on a regular basis.

2. Risk Assessment

2.1 The process of assessment looks at identifying all of the risks, evaluating them and prioritising them as high (risks requiring immediate action), medium and low risks. This is also about deciding whether a particular risk is acceptable or not, taking into account:

- the controls already in place;
- the consequence of managing risks or leaving them untreated; and
- benefits and opportunities presented by the risks.

2.2 Managers must ensure that they have assessed all areas of their department/section and roles. A standardised approach is taken across the organisation to analyse and measure risk; this is detailed in the Risk Management Policy and the Risk Management pages on Calsoft.

2.3 The key questions to consider in analysing any risk on a general risk assessment are:

1. What is the cause of the risk:

- What can happen?	- What has happened?
- How can it happen?	- How did it happen?
- Who could it happen to?	- Who did it happen to?
- How could risks occur?	- How did risk occur?

2. What is/could be the effect/s of the risk?
3. What is the resulting consequence to the Trust against its strategic objectives?
4. What is the likelihood of the risk occurring/reoccurring?
5. How could the consequence and or likelihood be reduced?
    - Are there any controls already in place to manage the risk?
    - Do these controls have any gaps?
    - What actions can be carried out to put more controls in place or close the current gaps?

2.4 A standard RAG ratting risk matrix is used to identify a risks score. This is calculated using two factors, the consequence of a risk multiplied by the likelihood of a risk occurring/reoccurring.

3. Identifying risks

There are many methods of risk identification within the organisation as highlighted in the Risk Management Policy. An “issue” is something that has already occurred and a “risk” is an issue that may or may not happen and could impact the Trust positively or negatively.

4 Entering Risks onto the Datix Risk Module (DRM)

4.1 In many cases it may be more appropriate to make a quick phone call rather than add a risk, however, if a risk needs to be added to the DRM please read on.

4.2 All managers and risk owners have access to the DRM once they have registered as a user and many sections/departments use a risk handler to help manage their risk management responsibilities - details on how to obtain a login can be found in the Risk Management pages on Calsoft

4.3 Risks are added to the DRM which has been designed to follow a standardised format that will collate all required elements of the risk - details on how to add a risk can be found on the Risk Management

4.4 The Risk Officer reviews all new risks that are added to the DRM to ensure continuity of formatting and to provide a horizon overview of the risk management system, including themes and trends . Notification will be provided via the DRM when the risk has been approved onto the system.

4.5 If a new risk has a current score of 15 or higher it will be marked within the DRM as a “Potential Corporate Level Risk (Being validated)”, this does not affect its approval to the system, it just highlights that the risk will be following the process for high level risks, as detailed in appendix 1.

4.6 When a “Potential Corporate Level Risk” has been approved by the Executive Team as a

"Corporate Level Risk" (CLR) it will be included in the "Board Assurance Framework" (BAF). In order to facilitate this, the Risk Officer will request assurances and potential assurances for the controls in place on the risk from the Risk Owner.

4.7 Linked risks, the DRM facilitates the linking of risks and incidents, it is good practice to record the linked risks / incidents, DRM ID No and Title in the linked records "Risk Description" for continuity reasons if this facility is used.

NB: Linking to a closed risk for purposes of continuity is also encouraged.

5 Reviewing Risks on the DRM

5.1 It takes time to plan and implement change. A robust monitoring and review process is essential to ensure action(s) are followed through to completion and that priorities are re-assessed. It is crucial when undertaking these assessments and reviews that details of when these were carried out and by whom are recorded. The DRM is a tool that facilitates these requirements.

5.2 Continuous monitoring and reviewing of risks ensures that new risks can be detected and managed, action(s) are implemented, and managers and stakeholders are kept informed.

The availability of regular information on risks can assist in identifying themes and trends, likely trouble spots or other changes that have arisen.

5.3 The current risk score will determine how often this risk should be reviewed.

Current Score	RAG Rating	Expected level of Management	Review period
15 to 25	Red	Board /Executive Team / Directorate	3 Monthly or sooner if new or significant information is forthcoming.

9 to 14	Amber	Directorate / ISU / Senior Manager	3 Monthly
5 to 9	Amber	Senior Manager / General Manager	4 Monthly
1 to 4	Green	General Manager	6 Monthly

5.4 Each step of the risk management process and the details of monitoring and reviewing risks must be recorded on the DRM. This enables the Risk Group to provide an extra level of assurance to the Board that risks are being managed effectively.

5.7 The NHSLA Risk Management Standards self-assessments and formal assessments will also provide extra assurance that risk processes are being effectively managed and will highlight any gaps. The risk management process and system of internal control is also formally reviewed annually by Internal Audit.

6 Communication and Consultation

6.1 Effective communication is key to ensuring risks are managed appropriately. Stakeholders should be involved and consulted throughout the process.

Key questions to answer are:

- Who needs to know?
- Who internally and externally needs to be consulted?
- Who is affected?

Appendix 1

Potential Corporate Level Risk Escalation Process

A potential corporate level risk is identified on the Risk Officers DRM dashboard.

The Risk Officer will set the "Risk Level" for this risk to "Potential Corporate Level Risk (Being validated)" and inform the relevant Senior Manager of the risk, asking for a validation of the risk and its score via the ISU/Department governance meeting.

Validated by Senior Manager

--No--

The risk description and score is adjusted by the Senior Manager or the Risk Owner.

Any changes made must be recorded in risks "progress notes".

Risk Officer will be made aware of this change via the DRM dashboard and the risk level would be changed accordingly.

Yes

The risk will then get a final validation at the ISUs Integrated Governance Group (IGG) Risk Officer will set the Risk Level to "Potential Corporate Level Risk (Validated)" and schedule the risk to be present to the next Risk Group meeting.

During the Risk Group meeting and the discussion concerning the risk, the Risk Officer will note the outcome, this could result in:

- The risk being approved as a "Corporate Risk" and adding to the Corporate Risk Register (CRR)
- The risk being approved and linking it to an existing "Corporate Level Risk" with the same theme.
- The risk being challenged by the members and feedback being provided to the risk owner and their senior manager. This risk should then be reviewed and changed as necessary, if still scoring as a "Potential Corporate Level Risk", this process will restart.

All outcomes of the Risk Group will be communicated to the Risk Owner, by the Risk Officer via the communications section of the DRM ensuring an audit trail exists.

Appendix 2

Themes for Identifying Risk

These can include, but are not limited to:

- General Risk Assessments where overall risk position for your area/dept need to be considered. This may include a review of multiple low level risks that could contribute to a bigger issue or risk e.g. failed Inspection.
- Introducing, changing or reviewing a process, system or service.
- As a result of an incident or near miss.
- PALS, Complaints and Claims reporting.
- Health and Safety inspection.
- Internal and External Audit.
- Compliance to legislation and/or a policy.
- Reports from assessments/inspections by External Bodies (including NSPA Monitor and other professional body guidelines).
- Surveys and Questionnaires.
- Issues arising from routine Patient and Public involved activities.
- Training.
- National reports & policies.
- Media.
- Central Alert System (CAS).
- Information risk (Electronic & Paper).
- Freedom of speech (Whistleblowing).
- Grapevine, Intuition, Observation (listening to hearsay and ad hoc comments, observing or becoming aware of potential risks or hazards – concerns should be discussed with your line manager).
- Safe Side / Trade Unions.
- Exit interviews with Staff.
- Backlog of Buildings Maintenance.
- Incident reports deemed as serious or untoward.

The above list is not exhaustive but raises awareness and identifies responsibility for formally addressing risk issues throughout the organisation and in all formats.