BrisDoc Patient care by people who care

NHS

Clinical Risk Management System

Version:	Owner:	Created:
1.1	Debbie Pople-Griffiths (Clinical Safety Office)	21/05/2025
Published:	**Approving Director:**	**Next Review**
12/03/2026	Rhys Hancock (Director of Nursing, AHPs and Governance)	12/03/2027

BrisDoc Patient care by people who care

NHS

Contents

Definitions

Further definitions can be found in the DCB0160 specification.

Term	Acronym	Definition
Clinical incident/Learning Event		Any event which has led to unintended and / or unnecessary harm to a patient. It does not include general software or hardware failures, which are managed through the general process for non-clinical incidents. These are also referred to as Learning Events within BrisDoc.
Clinical risk		Combination of the severity of harm to a patient and the likelihood of the occurrence of that harm.
Clinical Risk Management File	CRMF	Repository of all records and other documents that are produced by the clinical risk management process related to any Health IT System.
Clinical Risk Management Plan	CRMP	A plan which documents how BrisDoc will conduct clinical risk management of a Health IT System.
Clinical Risk Management System	CRMS	A set of deliverables and activities, defined by BrisDoc, to meet the requirements of DCB0129 and ensure clinical safety with respect to the development and modification of each Health IT System.
Clinical safety		Freedom from unacceptable clinical risk to patients.
Clinical Safety Case	CSC	Accumulation and organisation of product and business process documentation and supporting evidence through the lifecycle of a Health IT System.
Clinical Safety Case Report	CSCR	A report that presents the arguments and supporting evidence that provides a compelling, comprehensible, and valid case that a system is

Clinical Risk Management System

		safe for a given application in a given environment at a defined point in a Health IT System's lifecycle.
Clinical Safety Officer	CSO	The person nominated by BrisDoc who is responsible for ensuring the safety of a Health IT System through the application of clinical risk management. The CSO must hold a current registration with an appropriate professional body relevant to their training and experience. They also need to be suitably trained and qualified in risk management and understand principles of risk and safety as applied to Health IT Systems. The CSO ensures that the processes defined by the CRMS are followed.
Data Coordination Board	DCB	Committee that replaced the Standardisation Committee for Care Information (SCCI) on 1 April 2017. This committee is responsible for reviewing and approving the assurance of information standards.
Hazard		Potential source of harm to a patient.
Hazard Log	HL	A mechanism for recording and communicating the ongoing identification and resolution of hazards associated with a Health IT System.
Health IT System		Product used to provide electronic information for health or social care purposes. The product may be hardware, software or a combination.
Medical Device		A medical device can be hardware or software used to diagnose, prevent, monitor, or treat diseases or medical conditions without exerting a primary chemical action within or on the body.

Clinical Incident Management Log	CIML	Tool to record the reporting, management and resolution of clinical incidents/learning events associated with a Health IT System. For BrisDoc, Digital tickets are logged via the service desk or learning will be recorded and disseminated across the organisation, as a learning event.
Service Delivery & Improvement Group	SDIP	Performs the function of the Digital Clinical Safety Group
Structured What If Technique	SWIFT	A hazard assessment technique that uses brainstorming and structured discussions to identify risks.
Strategic Leadership Team	SLT	Persons who direct and control an organisation and have overall accountability for a Health IT System.

Introduction

This document outlines the Clinical Risk Management System[1] (CRMS) for BrisDoc Healthcare Services, subsequently referred to as 'BrisDoc' and it applies to all Health IT Systems that it implements and maintains. This CRMS defines how BrisDoc will integrate the DCB 0160 [Ref 1] and/or DCB 0129 [Ref 2] requirements and associated Clinical Risk Management (CRM) processes within existing Organisational Risk Management structures and processes.

This CRMS provides a framework that promotes effective risk management of known and potential Hazards in Clinical Software solutions. It is a critical assurance component of both DCB compliance, and the associated requirement to demonstrate that effective CRM has underpinned all Health IT system development, deployments, and life-cycle management activities.

In general, software suppliers such as CLEO, EMIS, Tortus and RiO are responsible for conforming to DCB0129 standards and providers such as BrisDoc are responsible for conforming to DCB1060 standards.

In most projects BrisDoc will be solely responsible for the activities and associated compliance for DCB 0160 only, however it is recognised that projects involving internal development may require BrisDoc to fulfil the obligations of DCB 0129 in addition to DCB 0160.

Limitations of the CRMS

The responsibility for the completion of the activities such as testing, training and business continuity planning, defined within this document fall to BrisDoc staff. The completion of the defined processes must be considered essential to the release of any Health IT System. The activities are designed to mitigate and / or minimise potential for actual and / or latent clinical hazards arising from the design, development, deployment, and use of IT Health Systems manifesting as actual patient harm.

[1] *Note: It is recommended that readers of this CRMS have read and understood the DCB 0160 and DCB 0129 Standards and associated Implementation Guidance* [Ref 3 & Ref 4] *prior to reviewing the document.*

Digital Technology and Clinical Safety

When delivering modern healthcare, digital technology, whether that be Health IT systems (HITS's), remote monitoring devices or clinical informatics guiding population health management, it is essential that Organisations follow structured methodologies to ensure any deployments are clinically safe and effective and free from unacceptable levels of risk.

However, Health IT Systems (HITS) have been linked to increased cognitive burden, stress and risk of burn-out in clinicians [Ref 5] and research demonstrates up to 75% of patient safety incidents related to digital technology use are preventable [Ref 6].

It is vital therefore that Clinical Safety is promoted and embedded within core governance channels and is appropriately recognised as a fundamental determinant of patient safety and effective care provision.

This Clinical Risk Management System (CRMS) for BrisDoc Healthcare defines the processes and procedures required by the Organisation to identify, assess and mitigate risk associated with both the manufacture (DBC0129) and implementation (DCB0160) of HIT Systems. The DCB Standards are mandated in law through the Health and Social Care Act 2012 [Ref 10] and this CRMS provides the operational framework for which BrisDoc Healthcare consider itself to meet these requirements.

The CRMS addresses all aspects of a HITS life cycle (design, development, implementation, maintenance, decommissioning) and details the processes required to ensure any actual or potential clinical risk associated with the system is mitigated to an acceptable level. It also builds upon the Risk Management Policy in order to ensure risk and governance are aligned.

Care Quality Commission

The Care Quality Commission address five key lines of enquiry when they appraise a Health or Social Care organisation [Ref 7]: Is it safe? Is it effective? Is it caring? Is it responsive to people's needs? Is it well-led? The impact of digital technologies can be felt across all five domains, whether that be through the utilisation of HIT Systems to improve care and reduce harm, or through our responsibility to ensure that the technologies we do use are as safe as possible.

To ensure CQC requirements are addressed, BrisDoc has created a Clinical Risk Management System specifically to address Digital Clinical Safety Concerns. It will deliver a Clinical Safety assurance process including Senior Clinical, Digital and Risk team membership to provide oversight for Health IT (HIT) systems currently in use, as well as those being considered for

procurement or imminent deployment. This will capture and monitor all digitally related incidents and take a thorough and proactive approach to near misses, whilst also serving as a structured communication channel between Governance, Operational and Clinical colleagues to ensure articulation and alignment of concerns and priorities. A key aim is to champion a proactive Digital Clinical Safety agenda in order to achieve seamless digital integration in clinical practice. Whilst it is often necessary to balance the risks of innovation and transformation within healthcare, the ambition is to ensure Clinical Risk Management is in the forefront of any HIT system change.

NHS Long Term Plan and Training

The NHS Long Term Plan [Ref 8], and the recently published NHS Long Term Workforce Plan [Ref 9] both set out the requirements for a digitally literate healthcare workforce. As stated by Health Education England 'As technology is evolving rapidly, we want the health and social care workforce to be fully capable, confident, and motivated in its use in the workplace. To achieve this, we need to develop a digitally literate health and social care workforce for today and the future'.

Indeed, if Health IT Systems are to be utilised safely and effectively within healthcare, it is imperative that all colleagues are digitally literate and competent with their use. Otherwise, we run the risk of unsafe or improper use, or the impact of non-adoption, leading to a credible threat to patient harm. At BrisDoc our staff undergo thorough 'Super-User' systems training with the aim of facilitating cascade learning, as well as providing a reciprocal communication channel.

From a Clinical Safety perspective, the ambition is to ensure all staff with HIT system responsibility will be formally trained in Clinical Safety Practice to ensure the principles of the risk management process are embedded into their work.

Clinical Risk Management System

The consideration and consolidation of the above-described threads have led to the development of a proactive and purposeful Clinical Risk Management System. In order to maximise engagement and produce meaningful outputs, the following areas have been addressed and/or restructured:

Risk Management Activity	Purpose
The Service Delivery and Improvement Group	Reciprocal communication and governance channel amongst Digital, Clinical, Technical and Patient Safety team members

	Proactive identification of safety concerns and ensure alignment between perceived digital risks and what is actually on colleagues 'worry-lists'.
Hazard Workshops	In the case of DCB0160 requirements, the initial Hazard Workshops will commence once the MVP product is available. A residual Hazard workshop will ensure all outstanding risks have been mitigated to an acceptable level before accepting the product for live use. All Hazard Workshops **MUST** be attended by Clinical, Operational; Governance and Systems lead in order to be quorate.
Templated documents (CRMP, CSCR, HL)	Standardised format for documentation which provides guidance and relevant examples of text, to support contributors.
Clinical Safety Gateways and Approval Form	Agreed criteria which must be met to proceed into the next stage of Clinical Safety activities. Non-compliance and exceptions to be documented and escalated, as required.
Residual Risk Acceptance Form	Standardised documentation to record Senior Responsible Officer (SRO)/Operational Owner awareness on key risk management activities, residual risk rating and transferred hazards. This document is the transfer of ownership point of known Clinical safety issues with any given software.

Underpinning Principles and Requirements of the CRMS

The CRMS has been produced by the CSO in conjunction with the Programme and Service Director and the Director of Nursing, Allied Health Professionals and Governance. The CRMS must be maintained throughout the life cycle of all Health IT Systems. The CRMS must be maintained and aligned with the most up to date version of any document referenced within it. The defined document owner is responsible for the maintenance of any such documents.

The CRMS forms part of the Clinical Risk Management File (CRMF) for products covered by DCB 0160 and DCB 0129. The CRMF for these products is held in a Shared drive. It contains all relevant clinical safety documentation and is managed by the Governance and Digital Teams.

The CRMS documents the key processes that will be undertaken by BrisDoc and Developers to ensure that Health IT Systems have been designed, developed, implemented, maintained, and decommissioned in a way that minimises any potential clinical risk that could arise through their application within clinical care environments or use for healthcare linked activities.

The CRMS has been produced to complement and build upon existing Organisational Risk Management processes as documented in the Risk Management Policy [Ref 11]. This enhanced framework provides a focused set of Clinical Risk Management (CRM) structures and activities that should enable BrisDoc and/or Development Teams to identify and mitigate System/product hazards. It will also support the organisation in effectively responding to clinical safety incidents arising from the deployments of, or changes to, any Systems used.

Existing procedures, processes, and governance structures currently undertaken as part of the established Risk Management frameworks will be utilised wherever possible for the purposes of fulfilling the needs of this CRMS and the overall CRM process. Evidence of CRMS integration with the organisational Risk Management policy must be captured and referenced as part of assurance processes.

Audience

The CRMS is intended to support all BrisDoc Team members and/or operational teams involved in the design, development, deployment, and maintenance of Health IT Systems and as such should be promoted and made readily accessible to all involved. This extends to any individuals managing clinical risks or patient safety that can be linked to digital systems, including post deployment incident review. The scope also includes individuals delivering digitally linked clinical products, or services.

The Director of Nursing, Allied Health Professionals and Governance in conjunction with the CSO will determine the members of the Leadership Team and other senior staff that are required to review, approve and support CRMS maintenance.

Scope

The CRMS covers the full life cycle of any given IT Health System, including but not limited to:

- (In-house) System scoping and design (DCB 0129)
- (In-house) System development and testing (DCB 0129)
- System release (DCB 0129) and System Install (DCB 0160)
- Hardware installation and Technical Integration (DCB 0160)

- System configuration (DCB 0160)
- Data migration (DCB 0129 and DCB 0160)
- System user acceptance testing (DCB 0160)
- System integration (DCB 0160)
- User Training (DCB 0160)
- System deployment (DCB 0160)
- System maintenance and upgrades (DCB 0129 and DCB 0160)
- Incident review and response (DCB 0129 and DCB 0160)
    - System decommission (DCB 0160)

If clarification is required as to whether a System falls within scope of this CRMS, this should be raised with the nominated Clinical Safety Officer (CSO) for confirmation. This nominated person provides clinical and organisational leadership in Healthcare IT Patient Safety.

Review

The CRMS will be reviewed at least every 12 months in line with policy management processes. This review will ensure that:

- The CRMS and Risk Management process remain aligned with applicable national and international standards and recognised best practice.
- The CRM process remains effective in mitigating clinical risks within the clinical settings and contexts within which each of the Health IT Systems are used.
- Working practices, the Risk Management Policy and the CRMS remain aligned.
- The CRMS is updated to reflect changes in Organisational Risk Management documentation and policy.
- The CRMS is updated to reflect the outcomes / address any issues identified through audit of risk management process.

Clinical Risk Management

The overall responsibility for DCB 0160 & DCB 0129 compliance and the CRMS resides with the Programme and Service Director. This section describes the individuals in BrisDoc who have

clinical risk responsibilities and the governance structures that are in place to manage clinical risks.

CRM is the central part of Clinical Safety Assurance and DCB 0160/0129 compliance. BrisDoc has integrated DCB 0160 and 0129 and linked CRM processes within existing organisation Risk Management policies and procedures, and embedded it into solution development, implementation, and maintenance practices.

Integration of robust, effective CRM processes within the Risk Management framework provides both a consistency in approach and an embedded culture of safety, enabling BrisDoc to deliver the following key aims in the context of CRM:

- Minimise the risk to patients whose care is supported/enabled by the Health IT System.
- Minimise the risk to users from the Health IT System.
- Provide effective quality and safety processes as part of a learning system that continuously improves Systems and Services.
- Ensure that BrisDoc meets is legal and moral obligations in providing safe, standards compliant Systems.
- Establish and embed robust, proactive mechanisms for responding to changing needs, System issues and evolving clinical risk potential.

The risk management process will be in line with the DCB 0160/0129 standard. **Figure 3** (below) summarises the key risk management steps:

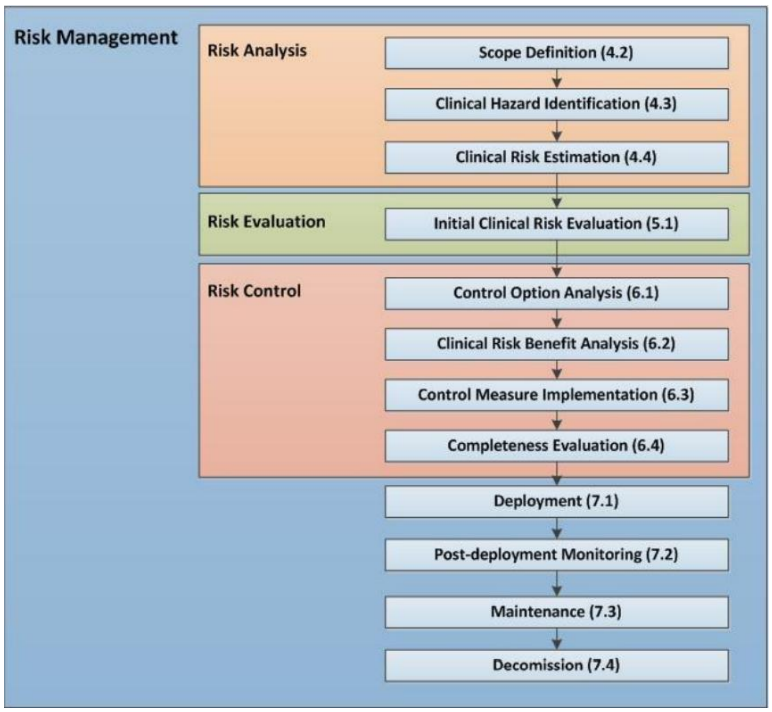


Figure 3: Risk Management process, extracted from the DCB 0160 Implementation Guidance

Clinical Risk Management Team

CRM principles and processes should be followed by all individuals involved with managing Health IT System design, development, implementation, assurance, review, and life cycle maintenance and as such CRM is not limited to the individual roles outlined below. Under the obligations of DCB 0160 and DCB 0129 the BrisDoc Board is ultimately accountable for standards compliance.

The following roles have specific responsibilities for clinical safety within the governance and management structures:

BrisDoc Board

- Executive and non-executive directors share responsibility for the effective management of risk. This includes:
    - Overseeing the delivery and effectiveness of the Risk Management Policy
    - Ensuring assurances clearly demonstrate that the Risk Management policy is being applied consistently.
    - Protecting BrisDoc's reputation through their full support and commitment to Risk Management activities and setting the organisational Risk Appetite

- In complying with its clinical risk management obligations (under the Health and Social Care Act 2012) in relation to Health IT Systems the Board **MUST** make available sufficient resources to fulfil its DCB 0160 and DCB 0129 obligations.

Programme and Service Director (Digital lead)

- Ensure that competent personnel are assigned from each of the specialist areas that are involved in developing and assuring Health IT Systems
- Ensure that the Programme has a nominated Clinical Safety Officer.
- Establish, document, and maintain processes to collect and review reported safety concerns and safety incidents involving Health IT Systems following deployment.
- Ensure safety related incidents involving Health IT Systems are reported to the Board & Clinical Safety Officer and resolved in a timely manner.
- Ensure competency and experience records for the personnel involved in performing the clinical risk tasks are be maintained.
- Ensure that DCB 0129 compliance and DTAC assessment is a mandatory requirement of any new Health IT System procurement.
- Maintain an identifiable record of safety incidents involving Health IT Systems, including their resolution.
- Establish at the start of a project a Clinical Risk Management File for the Health IT System.
- Complete/oversee any Risk/Benefit analysis required prior to deployment.
- Ensure that any recommendations/actions identified by the CSO as part of the Clinical Safety Case Report are actioned.
- Once a Health IT System has transitioned to a BAU status the Programme and Service Director will be by default be responsible for nominating a suitably trained and qualified CSO with the responsibility of:
    - Maintaining the Clinical Risk Management File for the life of the Health IT System.
    - Maintaining a Hazard Log for the Health IT System.
    - Maintaining a Clinical Safety Case for the Health IT System.
    - Maintaining a Safety Incident Management Log.
    - Ensuring that individuals are assigned to action the:
        - Implementation of the clinical risk control measures identified during the Control Option Analysis activities.

- Verification that each clinical risk control measure has been implemented.
- Verification of the effectiveness of each clinical risk control measure implemented.

Director of Nursing, Allied Health Professionals and Governance (Senior Responsible Officer)

- Will lead or delegate (with oversight) as needed, appropriately trained, knowledgeable individuals the:
    - Review and approval of the Clinical Risk Management System, working in conjunction with the Programme & Service Director and the nominated Clinical Safety Officer to ensure alignment with the Risk Management Policy
    - Review of clinical risk management processes at planned, regular intervals, communicating updates to the Board & Clinical Safety Officer.
- Establish roles and responsibilities within the organisation for the completion of defined clinical risk management and clinical safety related activities.
- Ensure robust, responsive mechanisms for review of safety related incidents involving Heath IT Systems as communicated by the Programme and Service Director.
- Review and approve Clinical Safety document templates, processes, guidelines, or policies.
- Establish and maintain Patient Safety and Clinical Risk Management governance processes within BrisDoc.
- Be responsible for:
    - Reviewing and accepting the project/programme residual risk and conclusions of the Clinical Safety Case Report on behalf of the organisation.
    - Ensuring that the clinical risks from all identified hazards have been considered and accepted on behalf of the organisation.

Nominated Clinical Safety Officer

- Oversee the implementation of the clinical risk analysis activities defined in the Clinical Risk Management Plan. Specific Compliance Responsibilities include but are not to:
    - A Clinical Safety Officer **MUST** approve Clinical Risk Management Plans.
    - A Clinical Safety Officer **MUST** approve any versions of Hazard Logs.
    - A Clinical Safety Officer **MUST** approve each Clinical Safety Case Report.

  - Clinical risk analysis SHOULD be carried out by a multi-disciplinary group including a Clinical Safety Officer.

- DCB 0160 and DCB 0129 mandate that the CSO MUST:
  - Be a suitably qualified and experienced clinician.
  - Hold a current registration with an appropriate professional body relevant to their training and experience.
  - Be knowledgeable in Risk Management and its application to clinical domains.
  - Make sure that the processes defined by the CRM process are followed.
- Review the Digital Technology Assessment Criteria (DTAC) submissions and escalation of deficiencies.
- Effectively complete DCB 0160/0129 documentation and activities.
- Implement the clinical risk analysis activities defined in the Clinical Risk Management Plan.
- Ensure all formal documents and evidence of compliance with the requirements of the DCB safety standards are recorded in the Clinical Risk Management File.
- Ensure any decisions made that influence the clinical risk management activities undertaken are recorded in the Clinical Risk Management File.
- Produce at the start of a project a Clinical Risk Management Plan, which will include risk acceptability criteria, for the Health IT System, aligned to this Clinical Risk Management System.
- Establish and maintain a Hazard Log, until such point as responsibility is transferred to the Programme and Service Director.
- Produce a Clinical Safety Case Report at each lifecycle phase defined in the Clinical Risk Management Plan, until such point as responsibility is transferred to the System Programme and Service Director.

Clinical Safety Competence & Training

The clinical safety activities described in this CRMS shall be undertaken by competent staff. Suitable training shall be undertaken by staff to maintain and expand their level of competence.

For a period of two years the responsibility for the DCB0160 deliverables will be contracted out to Infinitas Consulting Limited. During that time nominated BrisDoc personnel will undergo accredited Digital Clinical Safety Training.

A log of trained individuals will be available as and when this training is completed and will be stored in the Digital Clinical Safety SharePoint page.

Competency

All the staff shall be sufficiently competent for the roles and tasks which they are asked to undertake.

In assessing competency, the different functional roles required to fully discharge the obligations of the CRMS, and the necessary skills and knowledge needed for each, shall be considered. Primary functional roles and may include:

- Conducting discrete safety analyses (for example, FMEA) or defining the Hazard Risk Indicators for a particular project.
- Making a valid judgement on the safety of tasks, activities and techniques required for a given Health IT System to justify the comprehensiveness and completeness of the safety assessment and produce the safety argument with supporting evidence.
- Assurance of safety assessments of Health IT Systems. Performance of safety techniques and development of the safety argument for a particular Health IT System.
- Improving and refining the overall CRMS, for example, audit, process change, quality.
- Ownership and leadership, for example, ultimate safety accountability, culture change, influencing and strategic direction.

Training and mentoring

All nominated Clinical Safety Officers shall be required to undergo suitable training to develop, maintain or enhance their competency level. Such training can comprise:

- Internal training courses.
- Approved external training courses.
- Peer review

It is also essential that any nominated CSO maintains their Clinical Registration.

Organisational structure

The image representing the organisational meeting structure available in the Corporate Governance Framework shows the governance arrangements for Clinical Risk Management Assurance at BrisDoc and can be found by accessing the following link

Corporate Governance Framework – Radar

Risk Management Policy

Wherever possible this CRMS has been developed to align with the Risk Management Policy, inevitably through adherence to national standards requirements and recognised best practice there will be adapted variations required to meet the unique needs of Digital Clinical Risk Management. Reporting of incident and escalation of direct patient risk / harm potential should not deviate from standardised, embedded processes. The capture of risk is specific to the templates and context of system risk and/or digital transformation risk, however risk must be summarised and transferred to local risk registers in addition to Hazard Log production and maintenance.

Hazard Management

Hazard Identification

Hazard identification, documentation and mitigation will be conducted throughout the lifecycle of Health IT Systems as an embedded part of digital CRM. Hazards and the associated risk evaluation will be captured and updated via Hazard Logs, with each CSCR providing a consolidated summary of the risks identified.

Hazard identification will be applied at all stages of each Systems development and maintenance including but not limited to the following key life-cycle stages:

- Design Research (DCB 0129)
- (In-house) System scoping, prototyping, and design (DCB 0129)
- (In-house) System development, validation, and testing (DCB 0129)
- System release (DCB 0129) and System Install (DCB 0160)
- Hardware installation and Technical Integration (DCB 0160)
- System configuration (DCB 0160)
- Data migration (DCB 0129 and DCB 0160)
- System user acceptance testing (DCB 0160)
- System integration (DCB 0160)
- User Training (DCB 0160)
- System deployment (DCB 0160)
- System maintenance and upgrades (DCB 0129 and DCB 0160)

Clinical Risk Management System

- Incident review and response (DCB 0129 and DCB 0160)
- System decommission (DCB 0160)

Nominated CSOs conduct Hazard Identification Workshops (Hazard workshops), coordinated by the Programme and Service Director to identify potential hazards associated with the design and deployment and use of any given Health IT Systems. A nominated CSO will be responsible for facilitating such workshops and ensuring attendance from appropriate representatives. Typically, representatives from the following domains will be required:

- System managers / Asset Owners.
- Design and Development Teams.
- Testing, Training and Assurance Teams.
- Clinical Users
- Operational Users
- Supplier CSO

For Hazard workshops focusing on new / first time system reviews minutes will be taken or the meeting recorded, with a copy stored in the CRMF for each System review. The decision to formally take minutes or record the session will depend upon the scale/scope and complexity of the meeting/subject. If a solution is deemed not to be safety related, then this decision will be formally recorded.

If any third-party components are used to support any given Health IT System, then they will be considered in the scope of the hazard identification activities and subsequent risk assessment. Where none is used a positive declaration to this effect will be recorded in the minutes.

All identified hazards for a given System will be recorded in the HL for that System.

Risk Analysis

Risk Analysis will be conducted against the Health IT System in accordance with DCB 0160/0129 standard(s) and the specific requirements of the CRMP. The HL for each System will be updated to capture the Risk Analysis outputs.

Risk Evaluation

Risk Evaluation will be conducted against the Health IT System in accordance with DCB 0160/0129 standard(s) and the specific requirements of the CRMP. The HL for each System will be updated to capture the Risk Evaluation outputs.

The Reference table section of this document contains the following evaluation (Risk Assessment) criteria to be used within the context of CRM activities and DCB 0160/0129 compliance:

- Appendix A - Severity (Consequence) Descriptors.
- Appendix B - Likelihood (Probability) Descriptors.
- Appendix C - Clinical Risk Classification Matrix.
- Appendix D: Residual Risk Acceptance Categories.

Where possible all scoring systems are aligned with the Matrices used in the Risk Management Policy.

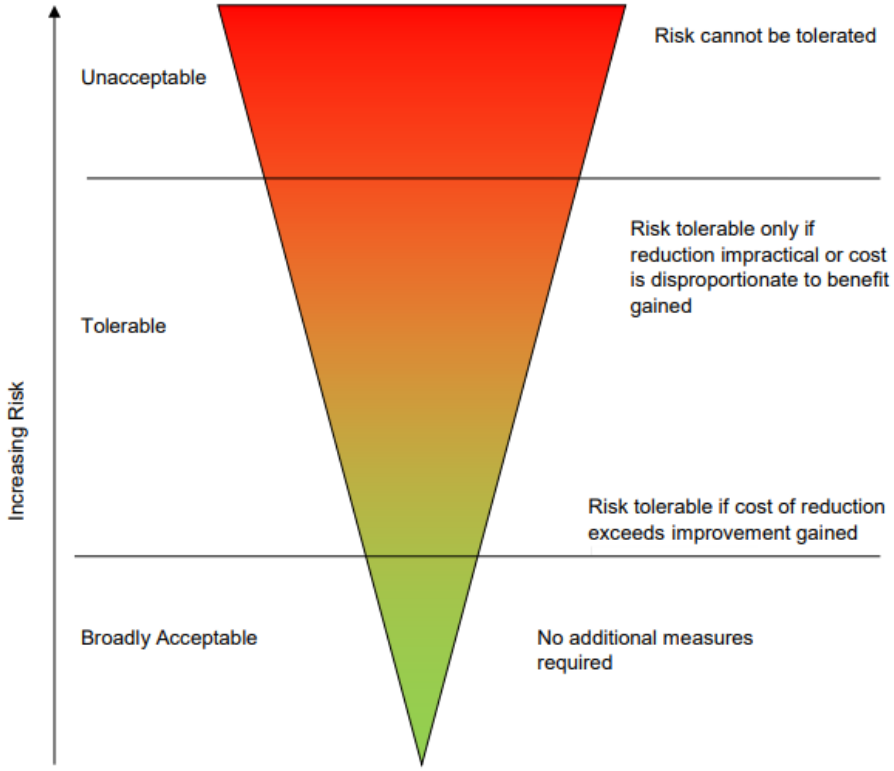
Risk Control

Where the initial Risk Evaluation is deemed unacceptable, further risk controls will be required. The Programme and Service Director will manage Health IT System risk in accordance with risk acceptance criteria.

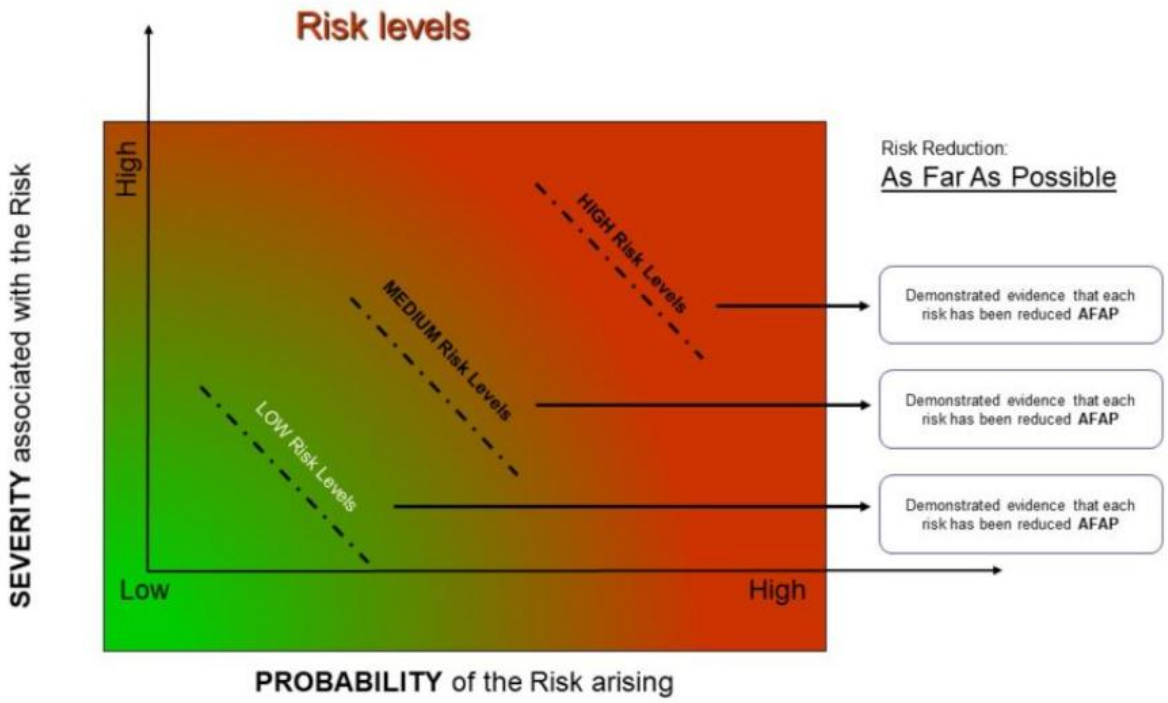
Details of the Risk Control Measures and evidence of their effective implementation will be captured in the HL of the System.

Risk Acceptance

Clinical risk should be considered acceptable in Alignment with the Residual Risk Acceptance Categories. Where there is uncertainty over whether further mitigations could or should be applied the concept of ‘As Low As Reasonably Practicable’ should be considered. This should weigh up the actual ability (technical practicability) to apply further mitigations vs the cost (economic practicability) of further mitigations, as illustrated below:



For medical devices, the concept of 'As Far As Possible' must be used. In practice this means that risk reductions will be as far as possible without adversely affecting the risk/benefit ratio, therefore financial considerations should not compromise the safety of medical devices.



All decisions must include the CSO and be fully explained in the CSCR.

Risk/Benefit Analysis

Where the Residual Risk of a Hazard and/or the Project/Programme as a whole is undesirable or unacceptable any decision by the SRO / Programme and Service Director to proceed with deployment **MUST** be underpinned by a thorough, documented and approved risk benefit analysis. The CSO must support this process, but ultimately the accountability for any decision will reside with the SRO / Programme and Service Director. The decision to deploy in the presence of an undesirable or unacceptable level of risk should only be take in absolute exceptional circumstances, where the impact of non-deployment clearly presents a greater overall risk.

Deployment, Updates and Maintenance (DCB 0160)

All system deployments and updates must be underpinned by a valid CSCR, HL and CRMP which have been approved by the CSO and SRO. The CSO will be required to complete a CSC Residual Risk Acceptance Form [Ref 12], this must be signed by the either the SRO and/or the Programme and Service Director of the residual risk, if this can't be provided then a system release should not proceed. The CSC Residual Risk Acceptance Form serves as the primary mechanism for acknowledging residual risk acceptance and associated actions/recommendation from the CSO, by the operational leadership team (either SRO and/or Programme and Service Director). In addition to this an Operational Readiness Checklist [Ref 13] should be completed, this will not

only confirm CSO approval of the CSCR and SRO approval for release but also serves as a secondary mechanism to confirm the transfer of operational risk and mitigation ownership.

The CRMP must detail responsibilities in relation to ongoing system ownership and configuration maintenance. Maintenance activities would not routinely require HL or CSCR updates but should be considered and assessed in the overall CRM process. If maintenance activities are considered to affect the validity of the CSCR or associated risk evaluation or control, then the HL and CSCR must be updated and reissued with CSO approval.

New Developments and Release Management (DCB 0129)

Where BrisDoc is responsible for system development and new system releases all activities must all to the CRM activities defined in the CRMP in accordance with DCB 0129 responsibilities. This will include review and revision of the HL and CSCR, with associated CSO approval prior to making new releases available for deployment.

The CRMP must remain up to date with the scale, scope, and context of any intended system use. CRM activities must in turn be reflective of the intend usage or potential misuse of the system.

Incident Management

Clinical safety related incidents are dealt with through the same process as other incidents within the organisation, in line with the Risk Management policy the Director of Nursing, Allied Health Professionals and Governance & nominated Clinical Safety Officer have active roles in incident review and response, including both investigation and mitigation of potential IT software risks/causes and IT software role with mitigation of non-IT linked risks.

Issues with clinical systems are reported via the Digital Help Desk or Learning Event portal. Where any risk is related to Clinical Flows, this will be highlighted to the Programme and Service Director (Digital lead).

If incidents are flagged to anyone outside of these channels, it must be ensured that the incident is logged via the standard procedures.

All digitally related issues, near-misses and incidents will be logged via a Digital Ticket or Learning Event and reviewed within the Service Delivery & Improvement Group (SDIP).

The Incident Management Log collates the following information:

- Date
- Incident ID (if available)

Clinical Risk Management System

- Patient ID (if available)
- Incident description
- Raised by
- Issue / Near-Miss / Incident
- Priority status
- Category
    - Loss of system
    - IT issue
    - Human Error
    - Configuration error/change
    - Functional failure / flaw
    - Technical Failure
- Review / summary of actions
- Responsible individuals for actions / follow-up
- Link to report / Hazard Log
- Lessons learnt
- Open / Closed

DCB 0129 obligations

All incidents and risks raised that fall under DCB 0129 obligations will be tracked via an incident management log, as part of the IT Service Desk, with a prioritisation and mitigation process defined within the body of the solution CRMP. Individual DCB0129 compliant solutions may require an independent Incident Management Log to be established, depending upon the agreed solution support processes.

Clinical Risk Management File (CRMF)

A Clinical Risk Management File (CRMF) is established and maintained as part of DCB 0160/DCB 0129 requirements. The CRMF provides a single central stored and control mechanism for all documents and information generated throughout each System life cycle, from initial

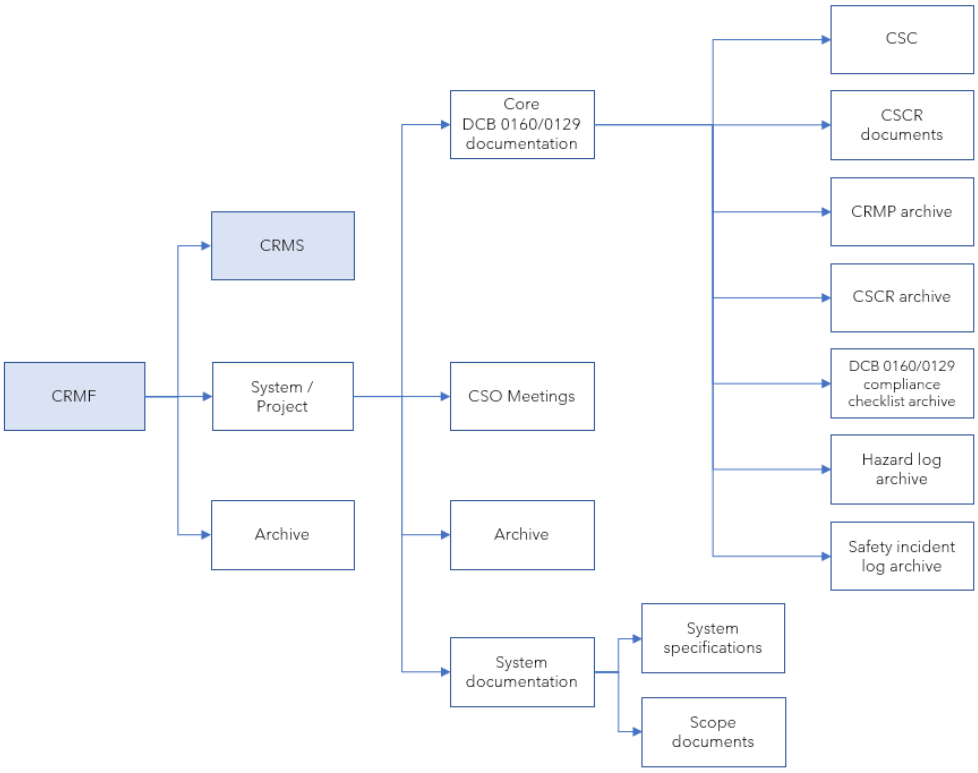
specifications and design, through to decommissioning. The CRMF is structured in such a way as to reflect the key components of standards compliance.

Figure 1 below (in Clinical Risk Management Deliverables section) demonstrates the key elements of the CRMF and outlines some of the documented evidence expected as part of CRM activities. The structure of CRMF is intended to support the CRM process by outlining key activities, structures, outputs, and processes, it provides systematic storage of documentation and information collated/produced throughout each System life cycle.

Effective document control, naming conventions, numbering systems and archiving processes must be maintained.

The CRMF can be accessed via a Shared Drive. An indicative structure of the CRMF is outlined below, in practice some folders will be accessed via shortcuts and/or links to other document stores:

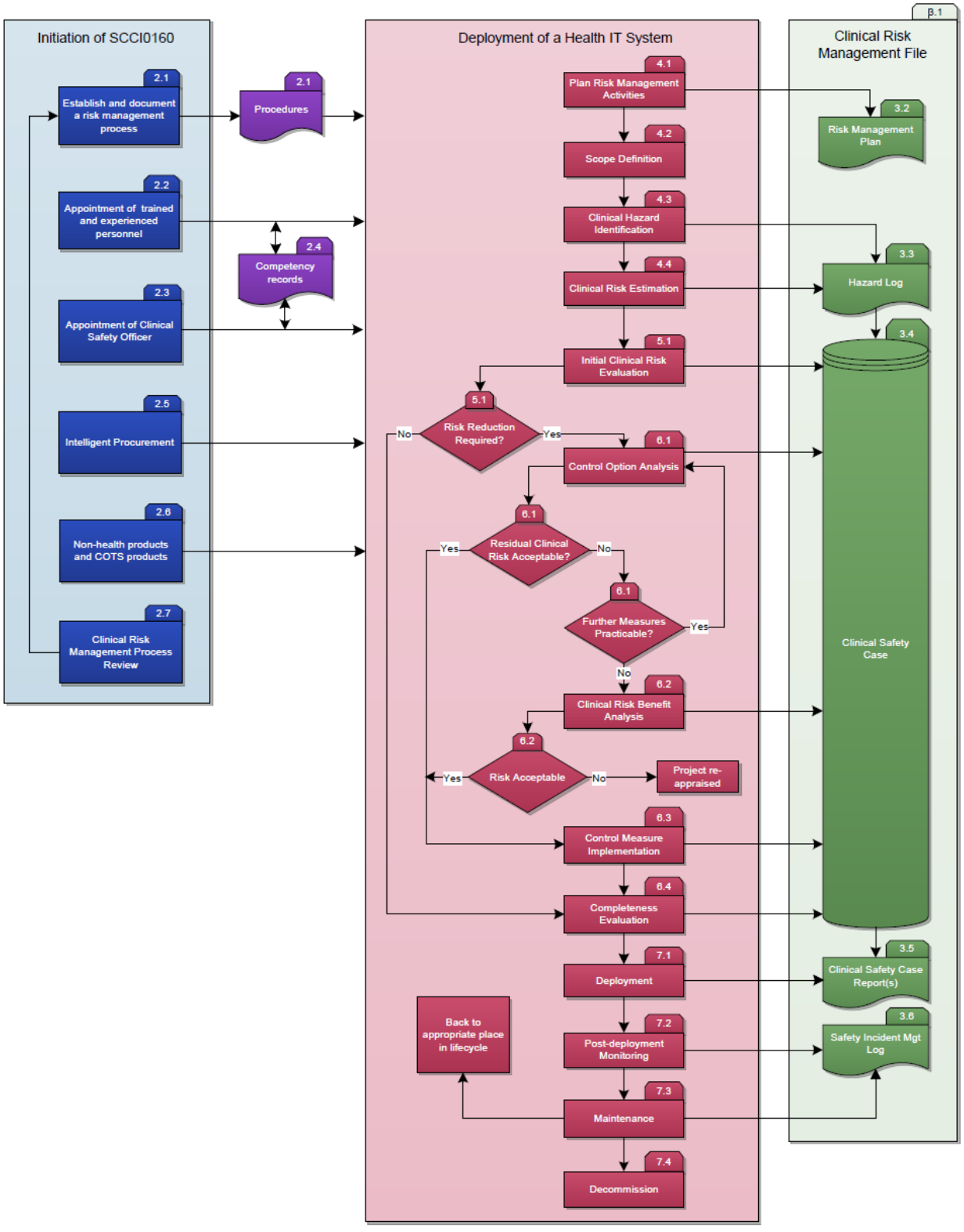
Figure 2 (above): CRMF structure



Clinical Risk Management Deliverables (Each Health IT System)

This section outlines the key CRM deliverables in relation to DCB 0160 and DCB 0129 compliance. These outputs will be produced and maintained throughout all Health IT System life cycles, as part of integrated CRM and QMS processes.

Figure 1 (below, extracted from the DCB 0160 standard): outlines DCB 0160 CRM activities and documentation.



The above diagram includes the key activities of the DCB 0129 process.

Clinical Risk Management Plan (CRMP)

The Clinical Safety Officer will provide a Clinical Risk Management Plan (CRMP) for the Health IT System however, the Programme and Service Director is responsible for its maintenance over the life cycle of each Health IT System, these documents are intended to cover all design, development, configuration, scope and deployment setting variations for each System.

The CRMP will be based on the BrisDoc CRMP template. This was created to standardise the approach to CRMP production, content, and formatting. This template should be adopted to the needs of each product.

The CRMP is also intended to document and communicate the CRM activities in relation to the specified Health IT System. The CRMP for each System is contained within the specified System's CRMF and is an essential part of compliance with the DCB 0160/DCB 0129 standards.

Each CRMP will cover the following CRM components:

- Definition and description of the Health IT System and the clinical context in which it will be used.
- Documentation of any variations to the standard practices and procedures defined in this CRMS.
- Identification of relevant procedures, policies and resources required to ensure effective and efficient CRM.
- Alignment and adherence to Governance, Quality and Project Management processes and requirements.
- Definition of the phases of the Health IT System life cycle and quantification of the clinical risk activities that are applicable to any specific phase.
- Documentation of the specific criteria that are to be used to estimate clinical risk and evaluate the acceptability of this risk.
- Identify and document key roles of responsibility and authority for each clinical risk activity and the resources needed to support each of these activities.
- Definition and documentation of those members of staff who can approve the safety documentation.
- Define the response to incidents, monitoring mechanisms and the safety review process.
- Document under what circumstance or periodicity the plan should be reviewed.

Clinical Risk Management System

DCB 0129 CRMP

Where BrisDoc is responsible for DCB 0129 compliance, the CRMP will reflect the additional CRM linked design and development activities undertaken. There should be a clear definition within the CRMP of the activities that fall under DCB 0129 compliance vs those that are for DCB 0160 activities.

Hazard Log (HL)

The Hazard Log (HL) is the standard mechanism for recording and communicating the on-going identification and resolution of hazards associated with any given Health IT System. Hazard Logs are organised to enable a systematic approach to the management of hazards and support the effective collation of Clinical Safety Case evidence[2]. Any new versions of a HL will:

- Incorporate new hazards, when identified.
- Record the mitigation of defined hazards through the implementation of clinical risk control mechanisms.
- Reference supporting evidence.
- Record the status of actions.

The HL will be based on the BrisDoc Hazard Log template. This was created to standardise the approach to HL production, content, and formatting. This template should be adopted to the needs of the project.

The CSO will provide a HL for the Health IT System; however, the Programme and Service Director is responsible for its maintenance over the life cycle of each Health IT System. Each HL will be maintained for the full life cycle of each System and is intended to cover all design, development, configuration, scope, and deployment setting variations.

The HL for a System can be found within the relevant section of the CRMF for a System. Each version of the HL must be approved by the nominated CSO.

[2] Note: **Mitigation evidence must be comprehensive**, robust, clearly aligned to the hazard and accurately documented. Risk must not be considered as reduced/mitigated unless a comprehensive body of referenced evidence is presented via the Hazard Log.

DCB 0129 HL

Where BrisDoc is responsible for DCB 0129 compliance, the HL will be utilised to capture the Hazards in the context of both a system manufacturer and system implementer. The Initial Risk section of the Hazard Log will focus on risk and mitigation through the lens of the manufacturer, and the residual risk section will focus on risk control through the lens of the implementing organisation.

Clinical Safety Case (CSC)

A Clinical Safety Case (CSC) will be established for each version of a Health IT System, as per DCB 0160/0129 requirements. The CSC contains CRM planning, activities and evidence presented as a comprehensive, concise, and consolidated safety argument that a Health IT System is safe for deployment within the defined context and scope. The CSC will be produced/revised as soon as practically possible after each System version is developed, the CSC will be presented via a Clinical Safety Case Report (CSCR).

The CSC documentation and evidence for a System can be found within the relevant section of the CRMF for a System.

Clinical Safety Case Report (CSCR)

The Clinical Safety Officer will issue the initial CSCR for the Health IT System, however the Programme and Service Director is responsible for ensuring its maintenance over the life cycle of each Health IT System including each released version of a Health IT System in alignment with key DCB 0160/0129 requirements, the CSCR will be updated throughout the full life cycle of any System and is intended to cover all configuration, scope and deployment setting variations.

The CSCR will be based on the BrisDoc CSCR template. This was created to standardise the approach to CSCR production, content, and formatting. This template should be adopted to the needs of the project.

The CSCR will communicate and evidence that hazards associated with the specified Health IT System have been identified and the associated risks evaluated and mitigated to an acceptable level. In doing so, the CSCR also evidences compliance with NHS England requirements which are set out in the DCB 0160/0129 Standard.

The CSCR for any given System can be found within the relevant section of the CRMF for a System. Each version of the CSCR must be approved by the CSO.

Clinical Risk Management System

DCB 0129 CSCR

Where BrisDoc is responsible for DCB 0129 compliance, the CSCR will be expanded to include all design and development related CRM activities and assurances, this includes mechanisms for post-market surveillance, incident response, system updates and release processes. There should be clear evidence available within the document of how these activities have been achieved, to demonstrate compliance.

Appendices

Table A - Severity (Consequence) Descriptors

Table A (below) defines the descriptors for the severity (consequences) associated with clinical hazards. These categories reflect single incidents, which may affect individual patients or several patients at once.

Severity (Consequence)	Score	Risk to patient, staff, business	Interpretation
Catastrophic	**5**	Multiple	Death
		Multiple	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term
		Corporate	Incident leading to death, non-delivery of business objectives, event which impacts on large number of patients/staff, multiple breeches to statutory duty, prosecution, national media coverage/total loss of public confidence, >25% over project budget/loss of >1% of budget, loss of contract, 1day loss of service.
Major	**4**	Single	Death
		Single	Permanent life-changing incapacity and any condition for which the prognosis is death or permanent life-changing incapacity; severe injury or severe incapacity from which recovery is not expected in the short term
		Multiple	Severe injury or severe incapacity from which recovery is expected in the short term
		Multiple	Severe psychological trauma
		Corporate	Major injury leading to long term incapacity, significant harm to patient, >14days off work, uncertain delivery of business objectives, enforcement action/multiple breeches of statutory duty, uncertain delivery of service due to lack of staff, national media coverage, 10-15% over project budget/loss of 0.5-1% of budget, >12hrs interruption to service.
Considerable	**3**	Single	Severe injury or severe incapacity from which recovery is expected in the short term
		Single	Severe psychological trauma
		Multiple	Minor injury or injuries from which recovery is not expected in the short term
		Multiple	Significant psychological trauma
		Corporate	Moderate injury requiring professional intervention, some harm to patient, 4-14days off work, unsafe staffing level, single breech of statutory duty, local media coverage/long term reduction in public confidence, >8hrs interruption to service, 5-

			10% over project budget/0.25-0.5% loss of budget, late delivery of business objectives.
Moderate	**2**	Single	Minor injury or injuries from which recovery is not expected in the short term
		Single	Significant psychological trauma
		Multiple	Minor injury from which recovery is expected in the short term
		Multiple	Minor psychological upset; inconvenience
		Corporate	Minor injury, minimal harm to patient, low staffing reduces service quality, breech of statutory legislation, local media coverage/short-term reduction in public confidence, >1hr interruption to service, <5% over project budget/loss of 0.1-0.25% of budget, minor impact on business objectives, >3days off work.
Minor	**1**	Single	Minor injury from which recovery is expected in the short term; minor psychological upset; inconvenience; any negligible consequence
		Corporate	Minimal injury, no harm to patient, no time off work, no/slight impact on business objectives, insignificant cost increase/financial loss, rumours, <30mins interruption to service, <1 day shortage of staff, no/minimal breech of statutory duty.

Table B - Likelihood (Probability) Descriptors

Likelihood (Probability) classifications and values are shown in table B.

Table B: Likelihood (Probability) Classification Measures

Likelihood Descriptor (Probability)	Likelihood Score (Probability)	Likelihood Frequency Descriptor considerations; a. How often might it / does it happen? b. Time frame? c. Will it happen or not?
Very High (Almost Certain)	**5**	a. Will undoubtedly happen / reoccur, possibly frequently b. Expected to occur at least daily c. 81% -100% of the time
High (Likely)	**4**	a. Will probably happen / reoccur but is not a persisting issue b. Expected to occur at least weekly c. 51% - 80% of the time
Medium (Possible)	**3**	a. Might happen / reoccur occasionally b. Expected to occur at least monthly c. 21% - 50% of the time
Low (Unlikely)	**2**	a. Do not expect it to happen / reoccur, but it is possible it may do so b. Expected to occur at least annually c. 6% - 20% of the time
Very Low (Rare)	**1**	a. This will probably never happen / occur b. Not expected to occur for years c. 0% - 5% of the time

Table C - Clinical Risk Classification Matrix

Table C combines Tables A & B in a two-dimensional matrix, used to compile hazard likelihood (probability) and severity (consequence) to yield a measure (or value) of clinical risk.

Table C: Clinical Risk Classification Matrix

Likelihood	Very High (5)	5	10	15	20	25
	High (4)	4	8	12	16	20
	Medium (3)	3	6	9	12	15
	Low (2)	2	4	6	8	10
	Very Low (1)	1	2	3	4	5
		Minor (1)	Moderate (2)	Considerable (3)	Major (4)	Catastrophic (5)
		Consequence				

Table D - Residual Risk Acceptance Categories

A key element of the clinical risk evaluation is to gain:

- An understanding of the specific risk levels.
- An understanding of where significant risks lie that may or may not subsequently be found capable of risk reduction to acceptable levels.

Table D below defines categories for the acceptance of a Health IT System derived residual risk associated with clinical hazards and sets out the actions required for residual risks.

Table D: Residual Risk Acceptance Categories

Risk Classification	Residual Risk Acceptance Category	Actions required for identified Residual Risks
1 - 4	Acceptable (Low Risk)	No further action required.
5 - 8	Acceptable (Moderate Risk)	No further action required where cost of further reduction outweighs benefits gained or where further reduction is impractical, otherwise apply mitigation options.
9 - 12	Undesirable (High Risk)	Attempts shall be made to eliminate or control, to reduce risk to a tolerable / acceptable level. Only acceptable where further risk reduction is impractical.
16 - 25	Unacceptable (Extreme Risk)	Mandatory elimination of hazard or application of additional control measures to reduce residual risk to an acceptable level.

Table E - Standard Hazard Log Structure

The table below contains a standard Hazard Log Structure and Headings:

Hazard Assessment	Hazard Description	Hazard - Potential source of harm to a patient.
		(Possible) Causes – Possible cause(s) that may result in the Hazard. These may be technical, human error, etc. Note: A Hazard may have multiple causes.
		Effect – The effect that the cause(s) have on the functioning of the system / process.
		Harm - Death, physical injury, psychological trauma and/or damage to the health or well-being of a patient.
Initial Risk Assessment	Existing Controls	Health IT (HIT) Design – Existing design features or configurations implemented in the Health IT System that mitigate against the Hazard and that are currently in place and will remain in place post implementation. This may also include specific tests designed to provide assurance of effective HIT design and/or configuration.
		User Training – Existing Training implemented or planned to be implemented that mitigates against the Hazard.
		Business Process – Existing Business Process implemented or planned to be implemented that mitigates against the Hazard. This should include any people or processes that increase Hazard / Cause detectability.
	Initial Risk Assessment	Severity – Measure of the possible consequences of a Hazard resulting in patient harm. Scored based on the descriptors shown in Appendix E
		Likelihood – Measure of the occurrence of harm based on existing controls. Scored based on the descriptors shown in Appendix C
		Risk – Initial Risk Rating Score calculated by multiplying the Initial Severity Score by the Initial Likelihood Score.
		Justification – Rationale for the Initial Risk Rating Score. This should include considerations of 'detectability' when justifying likelihood and any rationalisation of the most credible severity rating.
Residual Risk	Additional Controls	HIT Design – Identification of design features or configurations implemented in the Health IT System in order to provide mitigation against the Hazard. This may also include specific tests designed to provide assurance of effective HIT design and/or configuration.
		User Training – Identification of training to be implemented in order to provide mitigation against the Hazard.
		Business Process – Identification of any Business Process Changes implemented in order to mitigate against the Hazard
	Residual Risk Assessment	Severity – Measure of the possible consequences of a Hazard resulting in patient harm. Scored based on the descriptors shown in Appendix E
		Likelihood – Measure of the occurrence of harm based on the implementation of additional controls. Scored based on the descriptors shown in Appendix C
		Risk – Residual Risk Rating Score calculated by multiplying the Residual Severity Score by the Residual Likelihood Score.
		Justification – Rationale for the Residual Risk Rating Score

Related Documents

These documents provide additional information and may be specifically referenced within this document.

Ref	Title	Version / Date
Ref 1.	Data Coordination Board (DCB) 0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems Accessible via: DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems - NHS England Digital  Clinical Risk Management: its Application in the Manufacture of Health IT Systems - Specification	15 June 2023
Ref 2.	Data Coordination Board (DCB) 0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems Accessible via: DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS England Digital Clinical Risk Management - its A	15 June 2023
Ref 3.	Data Coordination Board (DCB) 0160: Step by Step Guidance Accessible via: Step by step guidance - NHS England Digital	4 August 2022
Ref 4.	Data Coordination Board (DCB) 0129: Step by Step Guidance Accessible via: Step by step guidance - NHS England Digital	4 August 2022
Ref 5.	Gardner RL, Cooper E, Haskell J, Harris DA, Poplau S, Kroth PJ, Linzer M. Physician stress and burnout: the impact of health information technology. J Am Med Inform Assoc. 2019	Feb 2019
Ref 6	Martin G, Ghafur S, Cingolani I, et al. The effects of preventability of 2627 patient safety incidents related to health information technology failures: a retrospective analysis of 10 years of incident reporting in England and Wales. Lancet Digit Health 2019; 1: E127-135	2019
Ref 7.	How we do our job - Care Quality Commission	13 May 2025
Ref 8.	NHS Long Term Plan » Overview and summary	2019
Ref 9.	NHS England » NHS Long Term Workforce Plan	22 April 2024
Ref 10.	Health and Social Care Act 2012 – Section 250 Accessible via: https://www.legislation.gov.uk/ukpga/2012/7/section/250	01.07.2022

Ref	Title	Version / Date
Ref 11.	BrisDoc Healthcare - Risk Management Policy Risk Management Policy v 4.3.pdf	V4.3 / 01.08.2025
Ref 12.	CSC Residual Risk Acceptance Form	V0.1(DRAFT)
Ref 13.	Operational Readiness Checklist	V0.1(DRAFT)

Change Register

Date	Reviewed and amended by	Revision details	Issue number
15/02/2025	DP-G	Initial Draft	0.3
21/02/2025	DP-G & DL	Following review and amendments to governance arrangement section and clarification of nominated Clinical Safety Officer role.	0.4
28/03/2025	DP-G & DL	Updating with further narrative	0.5
19/05/2025	DP-G	Finalised	0.6
20/05/2025	RH & DP-G	Final review and amendments made	0.7
21/05/2025	RH	Edit to incident categories and move of CRMF section. Approved Final Version	1.0
12/03/2026	DP-G	Minor formatting change page 9 and reviewed to ensure no major change required. CRMS remains valid.	1.1