INTEGRATION
ENGINEERING SAFETY MANAGEMENT

Engineering Safety Management
Hazard Management Procedure

Document Number: CRL1-XRL-O8-GPD-CR001-50002

Current Document History:

Revision:	Effective Date:	Author(s) ('Owner' in eB *)	Reviewed by: ('Checked by' in eB *)	Approved by:	Reason for Issue:
3.0	18/05/2016	G Sutherland S James	Chi Wong	J Bates	Following Periodic Review & update to accommodate changes to CSM process together with review of the PWHR Process and addition of Derived Safety Requirements module

Previous Document History:

Revision	Prepared Date:	Author:	Reviewed by:	Approved by:	Reason for Issue
1.0	17/08/11	C Bloxsome	K Harvey	M. Kilby	Updated following revision of the ESM System Safety Plan
2.0	11/10/12	C Bloxsome	K Harvey	M. Kilby	Following peer review

Revision Changes:

Revision	Status / Description of Changes
3.0	2 Year Review, together update following review of PWHR Process and addition of a Derived Safety requirements Module

Contents

1 Abbreviations

Abbreviations	
ALARP	As Low As Reasonably Practicable
AsBo	Assessment Body
CBA	Cost Benefit Analysis
CDM	Construction (Design & Management) Regulations 2015
CPFR	Crossrail Programme Functional Requirements
CRL	Crossrail Ltd
CSM	Common Safety Method
DeBo	Designated Body
DOORS	Database Object-Oriented Requirements System
DSRM	Derived Safety Requirements Module
EMC	Electromagnetic Compatibility
ESM	Engineering Safety Management
FMECA	Failure Modes & Effects Criticality Analysis
HAZID	Hazard Identification
HAZOP	Hazard & Operability Study
HRP	Crossrail Hazard Review Panel
LUL	London Underground Limited
MIRP	Maintenance Integration Review Panel
NNTR	Notified National Technical Rules
NoBo	Notified Body
PPE	Personal Protective Equipment
PWHR	Project Wide Hazard Record
RAM	Reliability, Availability and Maintainability
RAB (C)	CRL Rail Approval Board
RCA	Risk Control Action
RIR	Railways Interoperability Regulations
ROGS	Railways & Other Guided Transport Systems (Safety) Regulations 2006 (as amended)
RSSB	Rail Safety & Standards Board
SIF	Safety Issues File
SIL	Safety Integrity Level
SIRP	System Integration Review Panel
SMS	Safety Management System
TSI	Technical Specification for Interoperability
VPF	Value of Preventing a Statistical Fatality

2 Definitions

Definitions	
Accident	An unintended event or series of events that results in harm.
Actors	Actor is a term within the CSM Regulation [2] which refers to all parties which are directly or through contractual arrangements involved in the application of the CSM Regulation. This includes CRL, Designers, Contractors and Subcontractors.
ALARP /SFAIRP	The Health and Safety at Work etc Act 1974 (HSWA) places duties on employers in the UK to ensure that 'so far as is reasonably practicable' (SFAIRP) safety risks are reduced. When these duties are considered in relation to risk management the duty is sometimes described as a requirement to reduce risk to a level that is 'as low as is reasonably practicable' (ALARP). These terms therefore express the same concept in different context and should be considered to be synonymous. In assessing whether the risk associated with a hazard is ALARP, it is considered that ALARP is achieved by meeting a combination of one or more of the three Risk Acceptance Principles. Note: 'ALARP' is taken to mean tolerable and ALARP.
Assessment Body	The independent and competent person, organisation or entity which undertakes investigation to arrive at a judgement, based on evidence, of the suitability of a system to fulfil its safety requirements.
Consequence	The number of fatalities, major injuries, minor injuries, shock and trauma resulting from the occurrence of a hazardous event outcome. Consequences may range from benign to a multi-fatality accident.
Contractor	For the purposes of this document only, any organisation contracted to CRL which is required to, or carries out Design or Design and Build activity on behalf of the project. This definition is also specifically extended to include such Contractors appointed by the Canary Wharf Group and Berkeley Homes Ltd to build Canary Wharf and Woolwich stations respectively.
CRL System Safety Team	The System Safety Team constitutes the ESM competency core of CRL under the responsibility of the Head of System Safety who ensures that the members of the team have the competency and experience to carry out ESM responsibilities. The team is independent of the production process. Where applicable in this document and unless otherwise stated, 'Safety Team' refers to any individual within the team who has been assigned to the task by the Head of System Safety.
Designer	For the purposes of this document only, any organisation contracted to CRL which undertakes Design activity on behalf of the project. This definition is also specifically extended to include Designers appointed by the Canary Wharf Group and Berkeley Homes Ltd to design Canary Wharf and Woolwich stations respectively.
Duty Holder	A generic term which means in the context of Crossrail either the Infrastructure Manager / Station Manager or Transport Undertaking as defined under ROGs /

	Railway Undertaking as defined under RIR.
Engineering Safety Justification	A formal presentation of evidence, arguments and assumptions aimed at providing assurance that a system or product has met its safety requirements (including appropriate legislation and standards) and that the safety requirements are adequate to control the identified hazards.
Engineering Safety Management	The activities involved in making a system, product or other change safe and showing that it is safe. This involves considering the safety of the railway throughout the life of the change.
Hazard	A hazard is a condition that could lead to an accident.
Intolerable Risk	A risk which cannot be accepted and must be reduced.
Negligible Risk	A risk which is considered to be low risk and that is broadly acceptable
Proposer	Proposer is a term within the CSM Regulation [2] which refers to the person/ party in charge of implementing the change. CRL is the proposer under the CSM Regulation.
Reference system	A system proven in use to have an acceptable safety level and against which the acceptability of the risks from a system under assessment can be evaluated by comparison.
Risk	The rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm.
Risk Acceptance Principle	The rules used in order to arrive at the conclusion whether or not the risk related to one or more specific hazards is acceptable.
Risk Analysis	Systematic use of all available information to identify hazards and to estimate the risk.
Risk Assessment	The overall process comprising a risk analysis and a risk evaluation.
Risk Evaluation	A procedure based on the risk analysis to determine whether the acceptable risk has been achieved.
Safety	Freedom from unacceptable risk of harm.
Safety Analysis	Is the application of systematic theoretical analysis to estimate the potential risk of an accident from a system or activity.
Safety Issues File	A list of hazards maintained by the CRL Technical Directorate that are intended to be transferred to a future Duty Holder.
Technical Specification for Interoperability	Defined in the RIR as being “technical specifications for interoperability adopted by an EU institution in accordance with the Directive or the Conventional Directive or High speed Directive and in force by which each subsystem or part subsystem is covered in order to meet the essential requirements and ensure the interoperability of the rail system.”
Tolerable Risk	A risk which can be accepted so long as the risk has been reduced to ALARP. Risk that is assessed as ‘Tolerable’ does not necessarily indicate that the risk is ALARP.

3 Introduction

3.1 Purpose

3.1.1 The purpose of this document is to define the procedure by which the Crossrail Project identifies, manages and maintains a Hazard Record of safety risks associated with the future operational railway throughout the Project lifecycle, to which all Actors shall conform.

3.1.2 The Hazard Management Procedure supports the Crossrail's Engineering Safety Management (ESM) System Safety Plan [1].

3.1.3 The Central Section of the railway is to be authorised to be brought into service under the Railways Interoperability Regulations 2011 (RIR). The Hazard Management Procedure is intended to satisfy the hazard identification, risk analyses and evaluation requirements mandated in the European Union Regulation on Common Safety Methods (CSM) Risk Evaluation and Assessment [2].

3.1.4 Once the Crossrail railway has been accepted and is operated, the Hazard Record shall be handed over to the Duty Holders to be further maintained as an integrated part of their safety management systems.

3.2 Scope

3.2.1 This Hazard Management Procedure shall apply to the management of safety hazards identified at any stage of the Crossrail Project. The scope is the same as defined in Crossrail's ESM System Safety Plan [1].

3.2.2 This procedure describes: the roles and responsibilities for hazard management; the process for identifying and assessing hazards; the process for managing the hazard records via the Project Wide Hazard Record (PWHR) database; and the controls applied to that process.

3.2.3 The Construction (Design & Management) Regulations 2015 [3] (CDM) activities take an interest in the impact of the design on the safety of maintainers and neighbouring railways and the safety of workers during operation. However, compliance with the railway related safety Regulations in 1.1.3 are the primary means of assuring to the Office of Rail and Road (ORR) the safety of future railway operations, including maintenance, perturbed and emergency situations. For this reason the application of CDM and ESM processes will run in parallel. As the PWHR database will become a significant part of the demonstration that safety risks have been controlled, any CDM identified operational and maintenance hazards shall also be recorded in the PWHR, with an appropriate cross reference to the CDM Risk Register.

3.3 Procedure Revision

3.3.1 This document will be revised as necessary during the lifetime of the project so as to ensure that it remains relevant at all times.

4 Hazard Management Process

4.1 Overview

4.1.1 The PWHR is the key management tool used to record and track the operational and maintenance hazards identified during the Crossrail Project. The PWHR will be maintained throughout the life of the project to provide a record of all the Crossrail operational and maintenance safety hazards identified and the progress on resolving safety risks associated with these identified hazards. The PWHR will be used to track these hazards until they are closed. The PWHR utilises the Dynamic Object Orientated Requirements Management System (DOORS) database via a user-friendly front end developed by Comply Serve Ltd [4].

4.1.2 The hazard identification process for the railway systems and sub-systems will be undertaken by the Contractors following their individual System Safety Plans. These System Safety Plans will be accepted by Crossrail Limited (CRL) for conformance with its own System Safety Plan [1].

4.1.3 All hazards identified will be recorded by the Contractors in the PWHR. The PWHR will be used by CRL to assure the affective management of ESM within the contracts.

4.1.4 The Contractors will undertake suitable and sufficient risk assessment on their design to reduce the risk to a level that is tolerable and as low as reasonably practicable (ALARP). Reference to such assessments will be recorded by the Contractors in the PWHR.

4.1.5 The principle applied to the management of hazards throughout is the party best able to control the hazard will be assigned the task of closing it out. Where hazard or risk control actions (RCA) would be more appropriately managed via a different Contractor, the hazard and/or RCA will be transferred to another contractor via the PWHR (with the agreement of the other Contractor).

4.1.6 For those hazards that relate to design issues, their associated RCAs will be carried out by the relevant Designers. Safety evidence will be recorded by the Contractor to justify the safety risk has been reduced to a level that is tolerable and ALARP.

4.1.7 It shall be demonstrated that risks have been reduced to a level that is at least tolerable and ALARP by using one or more of the following CSM risk acceptance principles:

(a) The application of codes of practice (CoP)

(b) Comparison with similar reference systems (SRS)

(c) An explicit risk estimation utilising qualitative and / or quantitative methods (ERE)

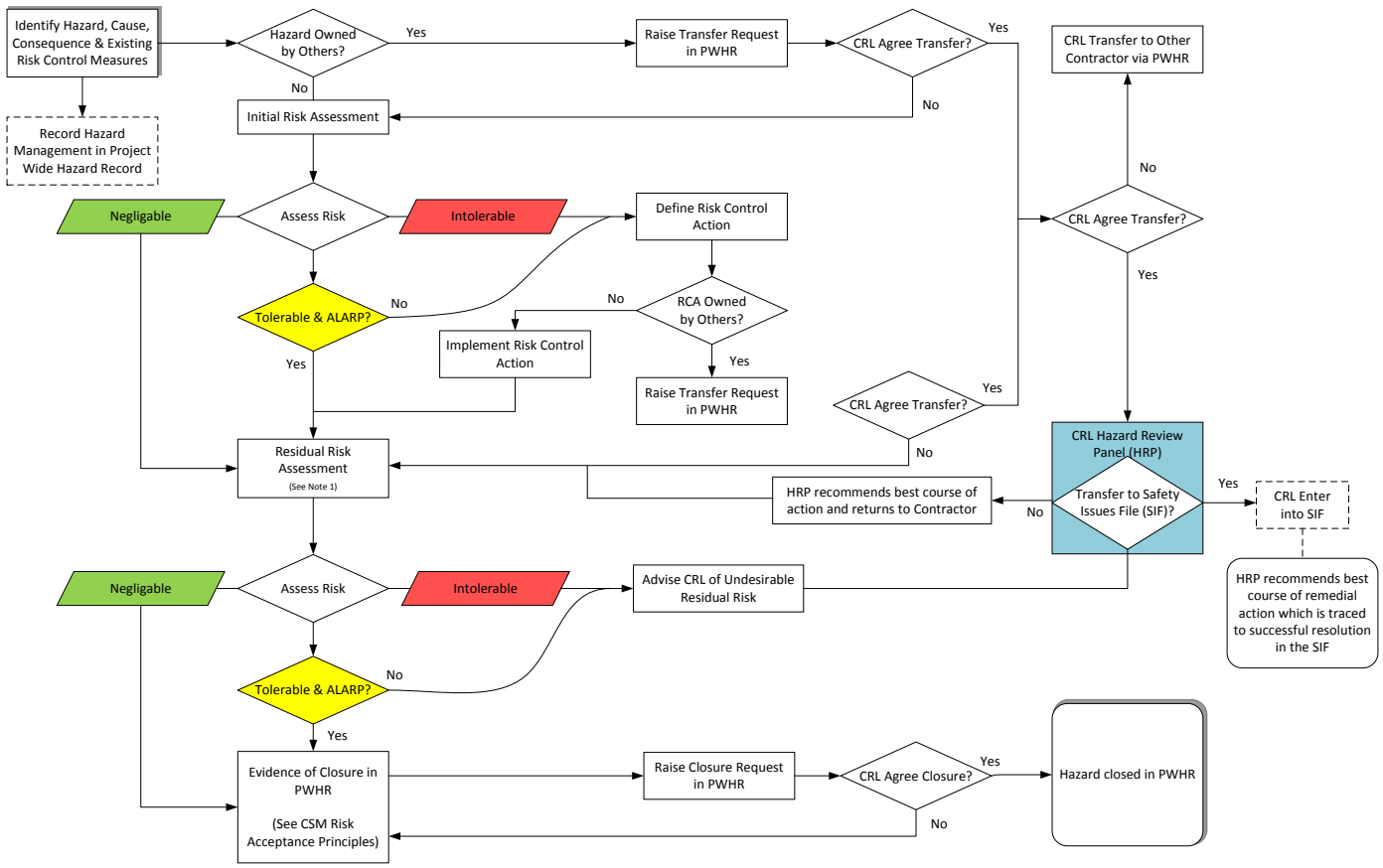
4.1.8 Once the hazard has been mitigated and sufficient safety evidence provided in accordance with the relevant risk acceptance principle, the hazard record will be requested resolved for the relevant project phase and then finally closed in the PWHR by the CRL System Safety Team.

4.1.9 For those hazards that relate to maintenance, operations and safety management system (SMS) issues the Contractors will prepare appropriate control measures (manuals, procedures, training, etc.), however, it will be necessary to transfer the responsibility for closure to the relevant Duty Holder. This shall be done in consultation with the Duty Holder and managed via the Safety Issues File (SIF).

4.1.10 The Hazard Review Panel (HRP) is a Crossrail (CRL) constituted body with responsibility for agreeing and reassigning Operations and Maintenance related hazards from the PWHR to the SIF.

4.1.11 An overview of the Crossrail project hazard management process is presented in the flowchart in Figure 1.

4.1.12 The references to CRL procedures and guidance for implementing this Hazard Management Procedure are given in the CRL ESM Reference Manual [5].



Note 1: If the Risk Acceptable Principle used is COP and / or SRS and totally encompasses the hazard, the residual risk assessment is not required. See the RSSB CSM Guidance.

Figure 1 - Hazard Management Flowchart Process

5 Roles and Responsibilities

5.1 Overview

5.1.1 The Crossrail project safety organisation is shown on the intranet Connect Online > Organisation home page.

5.1.2 The key responsibility of hazard management lies within the CRL Technical Directorate under the direction of the Head of System Safety. Figure 2 below shows the structure within the CRL System Safety Team.

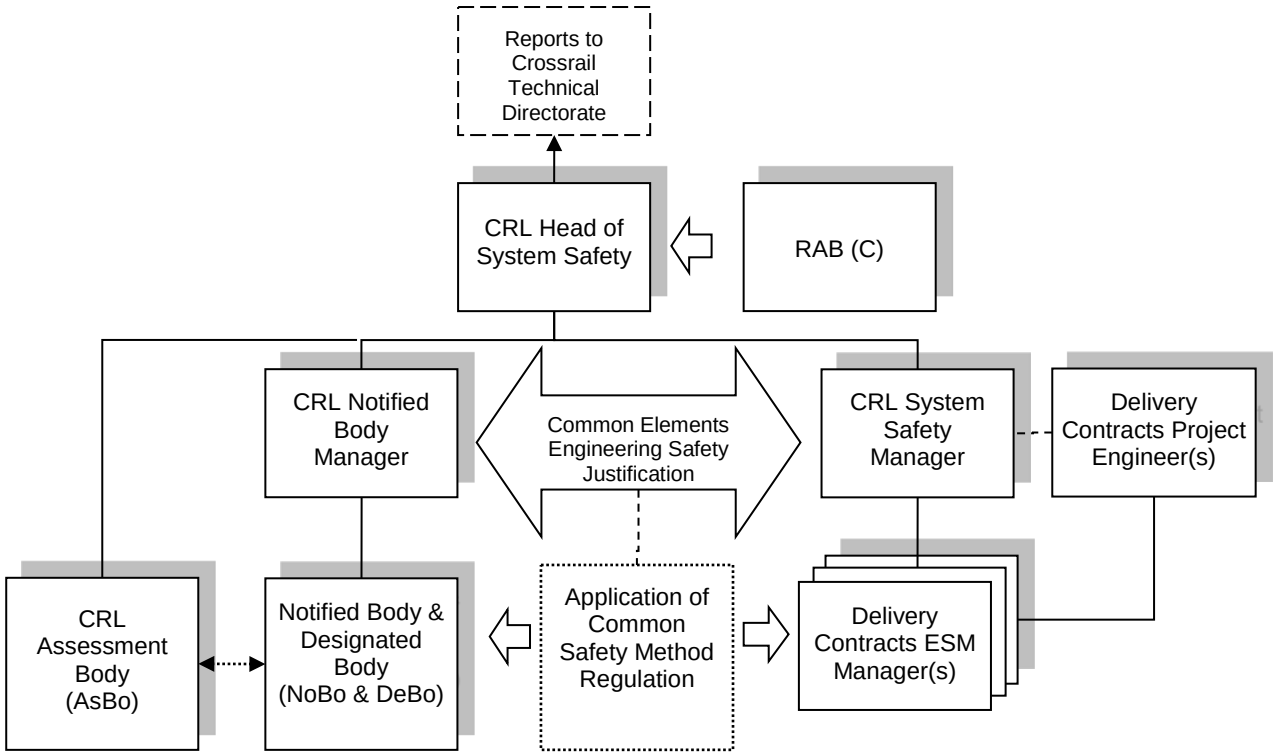


Figure 2 – Crossrail's System Safety Organisation

5.1.3 The key responsibilities for those roles and bodies responsible for hazard management are given in the following sections.

5.2 CRL Head of System Safety

5.2.1 The responsibilities of the CRL Head of System Safety include:

- Developing, implementing and maintaining the Crossrail ESM System Safety Plan [1] and to provide evidence of compliance with the relevant railway legislation including RIR, ROGS and CSM Regulation;
- Providing a framework for ESM activities to be undertaken by the Designers;
- Reviewing System Safety Plans developed by Designers;
- Acting as a point of contact for the client and stakeholders for all ESM issues and liaising with Designers;
- Managing the development of the PWHR [4];
- Having overall control of the PWHR and the strategy for hazard closure;
- Chairing the HRP and responsible for managing SIF;
- Managing the independent Assessment Body (AsBo) in its assessment of conformity of CRL and its Contractors with CSM Regulation;
- Checking that the risk information in the PWHR is kept up to date by contributors;
- Checking that the Crossrail Project HRP is made aware of any assistance or support that is required;
- Liaising with and progressing issued identified at the Systems Integration Review Panel (SIRP) and the Maintenance Integration Review Panel (MIRP).

5.3 CRL System Safety Manager

5.3.1 The responsibilities of the CRL System Safety Manager include:

- Reviewing System Safety Plans developed by Contractors;
- Liaising with the Contractors Safety Engineers;
- Monitoring ESM activities undertaken by the Designers;
- Carrying out surveillance to check that the identification of operational risks is being undertaken by the Designers, including the tracking and close out actions needed to control those risks;
- Having overall control with full editorial rights to add entries and to modify entries in the PWHR;
- Responsibility for reviewing hazards and endorsing any change of hazard status and reporting to the HRP;
- Review the transfer of hazards and control measures e.g. operational procedures;
- Actively seeking to arbitrate on difficult safety issues and facilitate appropriate transfer of hazards between Design teams;
- Reviewing Safety Reports generated by the Contractors;
- Assisting in the management of the AsBo in its assessment of conformity of CRL and its Contractors with CSM Regulation.

5.4 CRL Notified Body Manager

5.4.1 The responsibilities of the CRL Notified Body Manager include:

- Managing the NoBo / DeBo in developing, maintaining and monitoring an overall plan to facilitate TSI/NNTR compliance of CRL and its Contractors in conformance with the RIR;
- Assisting in the management of the AsBo in its assessment of conformity of CRL and its Contractors with CSM Regulation;
- Leading the identification of the need for derogations against TSIs and the requirement for CRL specific NNTRs;
- Checking that the development of applications for derogations are robust;
- Reviewing Safety Reports generated by the Contractors;
- Supporting the management of the PWHR, including reviewing hazards and endorsing any change of hazard status.

5.5 Contractors

5.5.1 The Contractors are responsible for appointing a person(s) to carry out the following responsibilities:

- Discharging the ESM requirements of contracts including development of Engineering Safety Justifications;
- Cooperating with the CRL NoBo/DeBo/AsBo in providing the necessary evidence to confirm compliance with the RIR and CSM Regulations;
- Undertaking Hazard Assessments, including risk mitigation of the elements of the design that are the responsibility of their organisation;
- Keeping the records of the hazards within the design that are the responsibility of their organisation up to date in the PWHR [4];
- Identifying and Derived Safety Requirements and ensuring population of the Derived Safety Requirements Module within the PWHR;
- Liaising with the CRL Head of System Safety for all ESM issues.

5.6 CRL Hazard Review Panel

5.6.1 The Hazard Review Panel (HRP) is a Crossrail body responsible for:

- Reviewing hazards that cannot be mitigated by design and require a future Duty Holder to manage via operational rules and regulations and/or maintenance process to ensure that the hazard is and remains Tolerable and ALARP throughout the operational phase;
- The management of the Safety Issues File (SIF) (see Section 5);
- Reviewing and determining the appropriate action for hazards that remain intolerable after the proposed hazard mitigations have been implemented;
- Acting as Arbiter;
- Reviewing any areas of concern highlighted during ESM surveillance;
- Reviewing any safety requirement non compliances and confirming acceptability of the safety justification.

5.6.2 The HRP format and terms of reference are given in reference [6].

5.6.3 The decisions of the HRP are mandated upon Contractors.

5.7 CRL Rail Approval Board (RAB(C))

5.7.1 RAB(C) acts as the CRL Safety Review Panel for all central section assets and is responsible for:

- Review and acceptance of Product Safety Cases and Engineering Safety Justifications provided by the various contractors and issuing the appropriate Acceptance Certification;
- Review and acceptance of Safety Justifications provided from within CRL and subject to specific assurances, issue of the appropriate Acceptance Certification.

5.7.2 Appropriate representation from RfL, CTOC, LUL and NRIL are provided on this Panel.

5.8 Assessment Body

5.8.1 The AsBo is an independent organisation appointed by CRL and responsible for:

- An independent assessment of the correct application of the risk management process under the CSM Regulation [2];
- Preparing Safety Assessment Report(s) as required by the CSM Regulation.

5.8.2 Any duplication of work already carried out by the NoBo or DeBo in accordance with the CSM Regulation should be avoided.

5.8.3 The AsBo will provide an Assessment Report that sets out, as a minimum, their approach to assessment, key information requirements, scope, criteria and definitions, supported by such guidance and interpretation of the relevant legislation as necessary to enable all parties involved in the Process to fully understand the AsBo requirements. This will include acceptance criteria and examples highlighting best practice. Annex III of CSM Regulation EU 402/2013 provides the minimum requirements [2].

5.8.4 Independence of the AsBo. The AsBo will be taken to be fully independent of the Design and Assurance Processes if it is remains uninvolved in any single or specific decision within a given design or assurance process. I.e. the AsBo should at no time influence or participate in that process. This excludes the provision of guidance relating to best practice which is made generally available to any and all parties prior to and throughout the design and assurance processes. See Article 6 of CSM Regulation EU 402/2013 for summary [2].

6 Safety Analysis

6.1 Overview

6.1.1 As described in the ESM System Safety Plan [1], the Actors are required to use recognised safety analysis methodologies based on the processes described in the EC Regulation on Common Safety Methods for Risk Evaluation & Assessment [2]. Examples of recognised methodologies include those shown in the ORR Guidance to the EC Regulation [8], British Standards BS EN 50126 [9], BS EN50128 [10], BS EN50129 [11], BS EN 61508 [12] and LU 1-526 [13].

6.1.2 The EC Regulation Common Safety Method on Risk Evaluation & Assessment [2] represents good practice and shall be complied with.

6.1.3 The scope of the Contractor's engineering safety analysis shall consider a comprehensive range of safety issues such as interfaces, operation, human factors, normal conditions, degraded conditions, emergency conditions and credible fault conditions.

6.1.4 The demonstration that the Design is ALARP shall be achieved by either quantitative or qualitative argument based on control of risks in accordance with the EC Regulation Common Safety Method on Risk Evaluation & Assessment [2].

6.1.5 For those parts of the Central Section LUL stations (Bond Street Station, Tottenham Court Road Station, Farringdon Station, Liverpool Street Station, and Whitechapel Station) on the platform side of the platform screen doors, the RIR does not apply. The CSM Regulation is therefore not mandatory, however, it is adopted by the CRL Project as best practice.

6.1.6 The CSM Regulation identifies that hazards can be analysed and evaluated using one or more of the following principles:

A. The application of codes of practice (CSM Regulation [2], Annex 1, Section 2.3)

B. Comparison with similar reference systems (CSM Regulation [2], Annex 1, Section 2.4)

C. An explicit risk estimation utilising qualitative and / or quantitative methods (CSM Regulation [2], Annex 1, Section 2.5).

6.1.7 It is envisaged that typically the Actors will use a combination of these principles to show that the safety risks have been reduced to a level that is tolerable and as low as reasonably practicable (ALARP).

6.1.8 The general principles applicable to the risk management process are given in Annex 1, Section 2 of the CSM Regulation [2].

6.1.9 The Actors shall demonstrate that the system is compliant with existing safety requirements and / or derived safety requirements.

6.1.10 The Actors shall ensure that safety assurance requirements are fulfilled.

6.2 System Definition and Safety Requirements

6.2.1 The overall Crossrail Project railway system definition is defined by the following reference documents:

- 20100310 – Sponsors Requirements – v4.1.0 (unredacted) [21]
- Crossrail Programme Functional Requirements (CPFR) [22]
- On-Network Functional Requirements [23]
- Central Section RAM Requirements [24]
- Maintenance Principles [25]

- Demarcation Drawings Supplementary Notes [26]
- Central Section EMC Management Plan [29]
- Cybersecurity [TBA]

6.2.2 The system definition of the subordinate sub-systems, for which the various Actors are required to carry out the relevant risk assessments, are defined in Volume 2 (Scope) of each delivery Contract. The system definitions are confirmed in the Contract specific System Safety Plans of the Actors concerned.

6.2.3 The overall Crossrail Project requirements are specified in the CPFR [22]. The safety requirements are specified within the CPFR. The Contractors are responsible for preparing the Safety Requirements Specifications although Contractors may identify additional safety requirements as part of the overall system requirements. The PWHR has the facility to record Derived Safety Requirements identified as part of the mitigation measures process [20]. The Derived Safety Requirements will be managed by the Contractors through to the completion of the works by use of the Derived Safety Requirements Module (DSRM) in the PWHR. The compliance status of the contract and derived safety requirements will be recorded within the Engineering Safety Justifications [27] for the relevant systems.

6.2.4 Should there be a non-compliance with a Safety Requirement, the non-compliance would need to be justified via risk assessment and recorded in the PWHR, DSRM and the Safety Requirements Specifications. These issues will be dealt with via the Hazard Review Panel.

6.2.5 There are no other safety level requirements set for the CRL railway (other than compliance to statutory requirements) and there is no apportionment of safety levels across the different subsystems and equipment. This is further explained in the CRL System Safety Plan [1].

6.2.6 Depending on the system, the Contractors may be required under the CSM Regulation to undertake a full qualitative and / or quantitative safety analysis in support of explicit risk estimation. In this case, the Contractors shall prepare a Safety Integrity Level (SIL) Requirements Report to recommend the system safety performance requirements against which the quantitative safety analysis will be evaluated. The identification of appropriate SILs is the responsibility of the Contractors, and shall be in accordance with the requirements of BS EN 50126 [9] and BS EN 61508 [12].

6.3 Hazard Identification

6.3.1 Contractors are responsible for identifying hazards, maintaining records of them in the PWHR and tracking progress of hazard close out. If the CRL System Safety Team accepts evidence for resolution and closure, the hazard status will be revised to “Request Resolved for Design / Installation / Energisation / Dynamic Testing / Trial Running” or “Request for Closure”. Only the CRL Safety Team can assign the “Resolved” or ultimately “Closed” status and therefore close a hazard record.

6.3.2 Hazard identification will take a variety of forms depending upon the function under review. Designers may undertake structured brainstorming sessions as well as reference to existing hazard identification for railway operations. Where appropriate other techniques such as FMECA and the HAZOP process shall be employed. Hazards identified during informal sessions are also valid. When a programmed hazard identification exercise has been undertaken, a draft report shall be produced and released to the participants and assurance representatives for comment within two weeks.

6.3.3 The future Duty Holders shall be consulted in the identification of hazards as appropriate.

6.3.4 Guidelines for preparing and undertaking structured workshops are given in the CRL Guidelines and Etiquette for Undertaking HAZID and HAZOP Workshop Guidelines [15].

6.3.5 All operational and maintenance safety hazards identified during the life of the project will be recorded in the PWHR.

6.4 Hazard Assessment

6.4.1 A systematic approach to hazard assessment using appropriate techniques shall be adopted in assessing hazards relating to the Crossrail Project. These hazard assessments shall be undertaken on an individual system discipline basis using system-specific information from the emerging designs.

6.4.2 The assessment will consider a comprehensive range of safety issues such as interfaces, operation, human factors, normal conditions, degraded conditions, emergency conditions and credible fault conditions of the Crossrail systems and subsystems.

6.4.3 As part of the hazard assessment, an initial, semi-qualitative risk ranking of the identified hazards will be undertaken to establish the broad levels of risk. Further details are given in Section 4.5. These will be logged in the PWHR by the Contractor.

6.4.4 The CSM risk acceptance principles identified in the following sections will be employed to satisfy the identified hazards. Where principles A or B only are employed the risks will not be analysed further. Where principle C, or a combination of A, B and C is employed a full risk assessment will be carried out in accordance with the CSM Regulation. The need for more detailed analysis (e.g. RAM, EMC, human factors, risk assessments) to support design will be established based on the outcome of the hazard assessment.

6.4.5 The risk frequency and severity categorisations to be used are shown in Tables 1 and 2 respectively. The risk classification is shown in Table 3.

6.4.6 All hazards are to be assessed in terms of frequency of a hazardous event and severity both at the inherent level, i.e. before any RCAs and at the residual level, i.e. after the RCAs have been carried out.

6.4.7 Where risks are identified and categorised as Intolerable or Tolerable, either changes to the design will be identified and evaluated, or procedures may be required to reduce the risk to ALARP.

6.4.8 Where risks are categorised as negligible or low, those risks will be considered broadly acceptable, subject to managing the risks at that level.

6.4.9 The Crossrail process for carrying out comparative risk assessments as part of optioneering of different design proposals considered on the Crossrail Project is given in reference 16 and section 6.9 below.

6.5 Codes of Practice (CSM Principle A)

6.5.1 The regulation defines a code of practice to mean “a written set of rules that, when correctly applied, can be used to control one or more specific hazards.” In order for codes of practice to be used for risk evaluation, it must:

- Be widely acknowledged in the railway domain (e.g. TSIs, European or British Standards, Railway Standards, etc.). If this is not the case, the codes of practice will have to be justified and be acceptable to the assessment body;
- Be relevant (the code of practice has been successfully applied to control the identified hazards of a system effectively in similar situations) for the control of the considered hazards in the system under assessment;
- Be publicly available for all who want to use them.

6.5.2 In many cases only a subset of the safety measures within the code of practice being referenced would be applicable to a given hazard. Therefore, the ensuing SR to control the hazards might reference only a specific clause or set of clauses of the code of practice.

6.5.3 When applying this principle, the simplest case is when safety measures from the code of practice completely control the hazard and the code of practice is fully complied with. This should then be added and become traceable to a SR.

6.5.4 The regulation also allows a hybrid approach. If safety measures from codes of practice cover most but not all of the risk associated with the hazard, then the principle may still be used, provided that one or more of the other principles is used for the parts of the risk which are not covered.

6.6 Similar Reference System (CSM Principle B)

6.6.1 The idea behind the "comparison with reference system(s)" principle is straightforward: one compares a new system against an existing "reference system" which is known to be associated with a level of risk which would be acceptable. The similarity of the reference system to the new system is considered, and if the systems are sufficiently similar (see criteria below) that there is no additional risk associated with the new system, then the risk from it is considered acceptable. The safety measures from the reference system will be adopted by the new system as SR.

6.6.2 The minimum requirements that a reference system must meet:

- It has already been proven in-use to have an acceptable safety level and would still qualify for approval in the Member State where the change is to be introduced;
- It has similar functions and interfaces as the system under assessment;
- It is used under similar operational conditions as the system under assessment;
- It is used under similar environmental conditions as the system under assessment.

6.7 Risk Assessment (CSM Principle C)

6.7.1 The 'explicit risk estimation' principle is the only risk acceptance principle that explicitly invokes the ALARP principle. There was already considerable experience in the UK of explicitly evaluating risk using the ALARP principle before the regulation was introduced and this experience remains applicable in this context.

6.7.2 The ALARP principle is not associated with a threshold of acceptable risk, below which risk can be accepted and above which it cannot. Instead, it requires demonstration that no reasonably practicable options to reduce risk further exist.

6.7.3 The risk management process allows risks to be evaluated either qualitatively or quantitatively. Either approach can be applied to support an ALARP test. Qualitative should only be used for low-level, well understood hazards. Quantitative analysis should be required for:

6.7.4 Hazards where there is a big risk reduction (e.g. moving from intolerable to tolerable), i.e. a lot of reliance is being placed on the system for safety.

6.7.5 Hazards which have complex sets of causes or multiple accident scenarios.

6.7.6 Quantitative risk evaluation generally requires significant effort and significant statistical data and is not always required. It is often possible to reach robust decisions using qualitative methods, which is detailed further below.

6.7.7 Quantitative risk evaluation generally requires significant effort and significant statistical data and is not always required. It is often possible to reach robust decisions using qualitative methods, which are discussed in the next section.

6.7.8 For a straightforward hazard, the 'explicit risk estimation' principle may be applied qualitatively in the following manner:

- Identify the causes of the hazard, and document as a table or short explanation.

- Identify the possible consequences of the hazard and the factors that affect those consequences, and document as a table or short explanation.
- Identify the existing safety measures which control the hazard.
- Identify the practical additional safety measures which might be implemented to control the hazard further.
- Review the additional safety measures, discard those that are judged not to be reasonably practicable and set safety requirements to implement those that are judged to be reasonably practicable.

6.7.9 Proceeding through these steps will lead to a robust decision, provided that:

- There are people with sufficient experience and knowledge involved in each step; and
- There is consensus that the hazard is understood such that the results of each step can be reliably obtained from experience and knowledge.

6.7.10 The 'explicit risk estimation' principle may be applied quantitatively in the following manner (this is similar to the CBA as detailed in section 6.9 of this procedure:

- Identify the causes of the hazard.
- Identify the possible consequences of the hazard.
- Identify the existing safety measures and further safety measures which control the hazard and which it has been decided to implement. This is the baseline case.
- Use the information from the previous steps to create a logical description of the causal chains which may result in an accident, usually using one or more specialist notations and computer programmes. Estimate the likelihood of the events in these chains and derive the frequency with which accidents occur.
- Use these frequencies to quantify the risk associated with the baseline case as a statistical estimate of the harm incurred per year. That harm may include both fatalities and injuries, and conventions exist, for combining these into a single number. (One such convention results in a measure called 'Fatalities and Weighted Injuries' or FWI for short. Risk is then measured in FWI per year.)
- Identify all practical additional safety measures which might be implemented to control the hazard further.
- For each safety measure, repeat steps 4 and 5, allowing for the effects of this safety measure, in order to estimate the reduction of risk resulting from the safety measure. The decrease in risk is compared with the increase in cost. Industry-standard benchmarks exist for deciding whether the option is reasonably practicable or not.

Table 1 Hazardous Event Frequency Definition

Frequency Category	Classification Term	Time frame	Midpoint Frequency Estimate	Description
5	Frequent	Less than a year	1 in 6 months	The event is likely to occur frequently (probably on a daily basis)
4	Probable	1 year to 10 years	1 in 5 years	The event will occur several times and is likely to occur often
3	Occasional	10 years to 100 years	1 in 50 years	The event is likely to occur several times
2	Remote	100 years to 1000 years	1 in 500 years	The event can be expected to occur during the lifecycle
1	Improbable	1000 years or greater	1000 years	The event is unlikely to occur but may by exception occur

Table 2 Consequence Definition

Consequence Category	Classification Term	Description
1	Negligible	Non-reportable injury
2	Minor	Minor injury
3	Major	Major injury/multiple minor injuries
4	Critical	Single fatality/multiple major injuries
5	Catastrophic	Multiple fatalities

Table 3 Risk Classification

Frequency	Consequence				
	1	2	3	4	5
5	T	I	I	I	I
4	T	T	I	I	I
3	N	T	T	I	I
2	N	N	T	T	I
1	N	N	N	T	T

I = Intolerable (High risk that is unacceptable), T = Tolerable risk, (when reduced ALARP is acceptable), N = Negligible low risk (that is generally acceptable)

It should be noted that 'Tolerable' risk does not necessarily indicate that the risk is ALARP.

6.8 Methods of addressing hazards

6.8.1 Identified hazards shall be addressed in the following order of precedence.

1. **Eliminate the hazard** (e.g. by changing the design).
2. **Design to minimise the risk.** If it is demonstrated that 1 is not possible, a design should be chosen to reduce the risk to an acceptable level.
3. **Incorporate safety devices.** If it is demonstrated that 2 is not possible, then devices shall be used to reduce the risk to an acceptable level.
4. **Isolate people from the risk.** If it is demonstrated that 3 is not possible, then a design should be chosen to isolate people from the risk to reduce the risk to an acceptable level.
5. **Provide warning devices.** If it is demonstrated that 4 is not possible, then warning devices shall be used to adequately warn personnel of the hazard. Human factors analysis shall be required to ensure that the warning devices are correctly interpreted.
6. **Develop procedures and training.** If it is demonstrated that 5 is not possible, then procedures and training shall be used to reduce the risk to an acceptable level. Human factors analysis shall be required to ensure that the procedures, training are adequate.
7. **Develop use of PPE.** If it is demonstrated that 6 does not adequately reduce the risk, then personal protective equipment shall be considered in conjunction with procedures. Human factors analysis shall be required to ensure that the procedures, training and equipment are adequate.
8. **Provide warning signs.** If it is demonstrated that 7 is not possible, then warning signs shall be used to adequately warn the population at risk of the hazard. Human factors analysis shall be required to ensure that the warning devices are correctly interpreted.

6.8.2 The future Duty Holders shall be consulted in the identification of mitigation where it affects their existing or future safety management systems.

6.8.3 Following the mitigation of hazards through maintenance and operational regimes it will be necessary to transfer that responsibility for close out to a Duty Holder. This shall be managed via the PWHR and the Safety Issues File process [17].

6.9 Cost Benefit Analysis

6.9.1 Where it is appropriate Cost Benefit Analysis (CBA) will be carried out (based upon quantified analysis of collective risk) in support of demonstrating that risks have been reduced as low as reasonably practicable (ALARP).

6.9.2 The ORR's Internal Guidance on CBA in Support of Safety-related Investment Decisions [18] and RSSB's Taking Safe Decisions [19] may be used as guidance by designers for the factors to consider when undertaking CBA.

6.9.3 It is noted that a CBA can not form the sole determinant of an ALARP decision.

6.9.4 When undertaking CBA, the most up to date Value of Preventing a Statistical Fatality (VPF) shall be used.

6.9.5 The Crossrail process for carrying out comparative risk assessments as part of optioneering of different design proposals considered on the Crossrail Project is given in Reference 16.

7 Crossrail Project Wide Hazard Record

7.1 Overview

7.1.1 The PWHR has been developed to record and manage all identified operational and maintenance hazards for the Crossrail railway. It acts as the central control and electronic reference document providing traceability of the hazard management activities for the Crossrail project. It is the Hazard Record as defined in the CSM Regulation Article 3 (16) of EU 402/2013 [2].

7.1.2 The PWHR is a 'live' database to be operated throughout the project lifecycle. It will require a series of iterations during the project lifecycle, including the testing, commissioning and handover phases. Following completion of handover, the PWHR document will be formally closed as a project record.

7.1.3 The PWHR functions include:

- Detailing hazards;
- Maintaining a list of safety records and a chronological journal of entries;
- Providing traceability to all other safety documentation (e.g. FMECA, FTA, CBA);
- Collating evidence to justify that the design can be operated and maintained to a level that is tolerable and ALARP.
- Maintaining a record of traceability to Existing and Derived Safety Requirements within the control measures and hazard records.
- Maintaining the Derived Safety Requirements in the Derived Safety Requirements Module (DSRM).

7.1.4 The PWHR is populated by the Contractors following the PWHR Process [20].

7.2 Structure

7.2.1 The PWHR is managed through the use of a web based DOORS database system hosted by Comply Serve Ltd [4].

7.2.2 The database is fully accessible for editing by the CRL Head of System Safety and nominated representatives.

7.2.3 All of the approved users will be able to view the entire PWHR.

7.2.4 A journal will record all changes to the database.

7.2.5 Deletions to the PWHR by Contractors shall not be permitted.

7.2.6 The Derived Safety Requirements Module within the PWHR will hold all of the derived safety requirements as identified and populated by the contractors.

7.3 Project Wide Hazard Record Management Process

7.3.1 All hazards shall be recorded in the PWHR. This includes those hazards classified as having broadly acceptable risk.

7.3.2 When a hazard has been identified and entered into the PWHR it will have a default status of "New". It will remain as "New" until it has been reviewed by the CRL System Safety Manager or their representative and they have agreed it is a valid hazard.

7.3.3 All changes to the status of hazards will be endorsed and effected by the Crossrail System Safety Team or the HRP.

7.3.4 Once the hazard has been reviewed by the CRL System Safety Team, it will either be assigned an "Open" or "Duplicated" status. "Open" hazards will be actively managed by the Contractor. Where a

Duplicated status has been assigned a comment will be entered to indicate the duplicate hazard reference and no further action (on the duplicate hazard) is required by the Contractor.

7.3.5 The Contractor will undertake safety analysis and propose a suitable combination of planned risk control measures and any other Risk Control Actions (RCA) to reduce the risk to a tolerable level and ALARP.

7.3.6 When the Contractor identifies a existing control measure it will be linked to an existing Safety Requirement in the performance specification or equivalent [20].

7.3.7 When the Contractor identifies and RCA within its scope, a Derived Safety Requirement will be logged in the DSRM within the PWHR and linked to the Control Measure [20]

7.3.8 The Contractor will review all control measures and prepare the Risk Acceptance Principle statements in the Evidence of Closure column to support the ALARP argument for each project phase. The hazard record will then be assigned as "Request Resolved for Design / Installation / Testing / Commissioning" status for CRL review.

7.3.9 The planned risk mitigation measures and any other risk control actions will be reviewed by the CRL System Safety Team. Once the CRL System Safety Team have reviewed the safety justification and accepted the Contractors mitigation proposals the hazard record will be assigned a "Resolved for Design / Installation / Test / Commissioning" status.

7.3.10 Under the CSM Regulation the risk acceptability of the system under assessment is evaluated by using one or more of the risk acceptance principles (clause 4.1.7). It will be necessary as part of the evidence for closure for the hazard owner to explicitly state which risk acceptance principle(s) the hazard has been evaluated and document the relevant justification. For example, if the hazard is controlled by codes of practice, references to those codes must be stated from the Crossrail Standards Baseline. If another standard is used it must be endorsed by CRL in accordance with the Standards Management Procedure [28].

7.3.11 When all identified control measures and risk control actions within the Contractor's control have been "implemented" (i.e. the linked safety requirements existing or derived have compliance evidence) for the applicable project phase, and the RCSs outside of the Contractor's control have been transferred AND accepted by the 3rd party (i.e. another contractor, Crossrail or RfL), the NRP should update the "Evidence for closure" to "Request Resolved for Design / Installation / Energisation / Dynamic Testing / Trial Running". The CRL Safety Team can subsequently approve the "Resolved" status.

7.3.12 Under the CSM Regulation, it is the Proposer's responsibility to check that selected risk acceptance principle is adequately applied and that the selected risk acceptance principles are used consistently. As such, the hazard record and risk evaluation will again be reviewed by the CRL System Safety Team to demonstrate in the risk evaluation that the selected risk acceptance principle is adequately applied for all project phases. The hazard status shall then be changed to "Closure Request" by the Contractor. The hazard will only be considered for closure by the CRL System Safety Team once the testing and commissioning has been successfully completed and the appropriate documentation referenced within the PWHR. If the CRL System Safety Team accepts evidence for closure, the hazard status will be revised to "Closed". Only the CRL System Safety Team can close the hazard record.

7.3.13 Dependent upon the hazard the CRL System Safety Team may seek technical support from the appropriate CRL discipline engineer to confirm that the closure evidence is suitable and sufficient. For example, where hazards are closed by reference to codes of practice, this is confirmed by the relevant lead discipline engineer in a formal review of the PWHR.

7.3.14 If it is considered that the hazard or proposed action to resolve the hazard would be better undertaken by another party, then a transfer request should be proposed by the originator of the hazard for consideration by CRL. The status within the PWHR will be changed by the Contractor to "Transfer Request".

7.3.15 For those "Transfer Request" hazards to be mitigated by design by another Contractor, the Hazard Record entry will be transferred by the CRL System Safety Team to the other Contractor with their agreement. The original Hazard Record will be recorded as 'Transferred' and a comment will be entered to indicate to which party now owns the hazard. A new entry will be recorded in the PWHR for the other Contractor, the entry will be recorded as 'Open'. A comment will be entered to indicate that the hazard was originally managed by the 3rd party.

7.3.16 For those "Transfer Request" hazards that relate to maintenance, operations and SMS issues the Contractors will prepare appropriate control measures (manuals, procedures, training, etc). However, it will be necessary to transfer the responsibility for closure to the relevant Duty Holder. The Hazard Review Panel (HRP) will confirm that the control measures are acceptable and can be managed via the Safety Issues File (SIF). Once the hazard record has been transferred to the SIF the original Hazard Record will be recorded as 'Transferred' and a comment will be entered to indicate that the hazard is being closed through the SIF process and the SIF Unique No. referenced.

7.3.17 Transfer of specific control measure RCAs to other contracts (where part of the hazard control lies outside the contractors scope) will be undertaken in line with the PWHR Process [20]. The transfer, if accepted will provide linkage between Contractors' PWHRs so that Crossrail can trace where the control measure is being managed

7.3.18 Specific details of the PWHR process including the mechanism for access to the PWHR are given in the PWHR Process document [20].

7.4 PWHR Summary

7.4.1 A PWHR Summary will be issued at points deemed appropriate by the CRL Head of System Safety, to provide a reference point for the PWHR at a given point in time.

7.4.2 A PWHR snapshot should be provided by contractors at each gate and lifecycle stage to support the safety justifications.

8 Safety Issue File

8.1.1 The Safety Issues File (SIF) has been developed to collect issues that require to be addressed by the future Duty Holders in future Crossrail railway rules and procedures.

8.1.2 The issues raised in the PWHR will be presented at the Crossrail HRP and once accepted will be added to the SIF. The HRP may also reject an issue and return it to the Contractor for further design mitigation, or forward it on to others who are responsible.

8.1.3 The Safety Issues File is a 'live document' maintained by the CRL System Safety Team and managed through the HRP.

8.1.4 Actions are raised in the SIF to record the proposed implementation strategy; issues will be traced to successful resolution in the action tracker and closed only when the related actions are successfully resolved. This shall be done in consultation with the Duty Holder.

8.1.5 Details of the SIF Process are given in the Crossrail Safety Issues File (SIF) and Action Tracker Status Report [17].

9 Reference Documents

Ref:	Document Title	Document Number:
1.	Engineering Safety Management System Safety Plan	CRL1-XRL-O7-GST-CR001-00001
2.	EC Regulation EU 2015/1136 and EU 402/2013 on the common safety method for risk evaluation & assessment	N/A
3.	The Construction (Design & Management) Regulations 2015	N/A
4.	Project Wide Hazard Record DOORS database system by the hosting company Comply Serve Ltd, http://www.complyserve.com/	N/A
5.	Crossrail Engineering Safety Management Reference Manual	CRL1-XRL-O8-GML-CR001-50001
6.	Crossrail Hazard Review Panel Terms of Reference	CRL1-XRL-O8-GPS-CR001-50009
7.	RSSB, Engineering Safety Management Fundamentals and Guidance (Yellow Book)	Issue 4, 2007
8.	ORR Guidance on the application of the Common Safety Method for risk evaluation and assessment	Issued by ORR March 2015
9.	Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	BS EN 50126-1:1999, BS EN 50126-2:2007, BS EN 50126-3:2006
10.	'Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems	BS EN 50128: 2003
11.	'Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling	BS EN 50129: 2003
12.	'Functional safety of electrical/electronic /programmable electronic safety-related systems – Part 1: General requirements	BS EN 61508-1: 2003
13.	The Assessment and Management of Health, Safety & Environmental Risk	LUL 1-526 Issue 3 June 2009
14.	Crossrail Common Safety Methods Hazard Assessment Process	CRL1-XRL-O8-GPS-CR001-50003
15.	Guidelines and Etiquette for Undertaking HAZID and HAZOP Workshops	CRL1-XRL-O8-GPS-CR001-50010
16.	Crossrail Process and Format for Comparative Risk Assessments	CRL1-XRL-O8-GPS-CR001-50007
17.	Crossrail Safety Issues File (SIF) and Action Tracker Report	CRL1-XRL-O8-LLG-CR001-50001

18.	Internal guidance on cost benefit analysis (CBA) in support of safety-related investment decisions. http://www.rail-reg.gov.uk/upload/pdf/risk	N/A
19.	RSSB, Taking Safe Decisions	GD-0001-SKP, 2008
20.	Project Wide Hazard Record Process	CRL1-XRL-O8-GPS-CR001-50013
21.	Sponsors Requirements Version 4.1.0	CR-XRL-O6-GPD-CR001-50002
22.	CPFR Baseline	CRL1-XRL-O8-RSP-CR001-50015
23.	On-Network Functional Requirements	CRL1-XRL-O8-RRS-CR001-00001
24.	Central Section RAM Requirements	CRL1-XRL-O8-RRS-CR001-00002
25.	Maintenance Principles	CRL1-XRL-O8-XTC-CR001-00002
26.	Design Demarcation Boundaries Drawings Supplementary Notes	CRL1-NRI-N2-RGN-CRG04-00008
27.	Crossrail Format and Process for Engineering Safety Justifications for Systems	CRL1-XRL-O8-GPS-CR001-50004
28.	Standards Management Procedure	CR-XRL-N2-GPR-CR001-00013
29.	Systems Engineering - EMC Management Plan	CRL1-XRL-O8-STP-CRG03-50003

10 Standard Forms / Templates

Ref:	Document Title	Document Number:
A.	None	
B.		