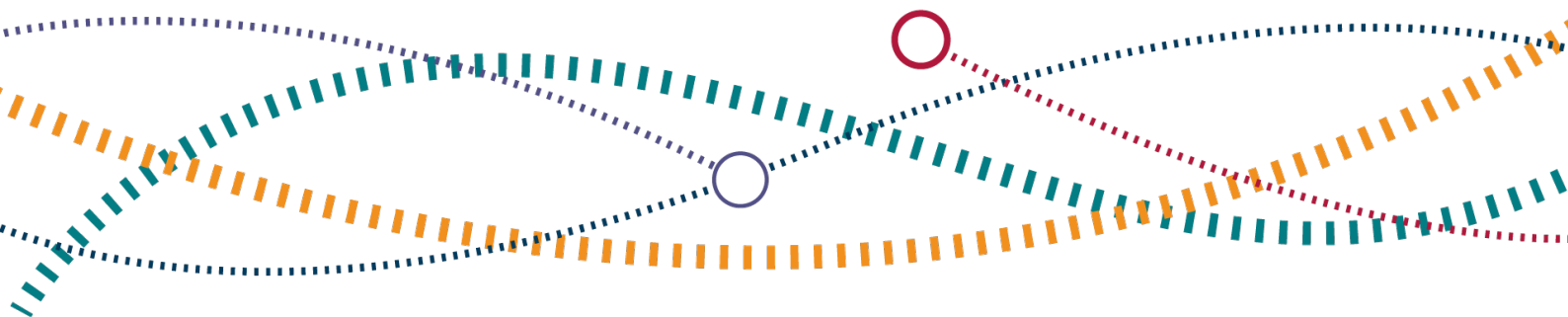




Common Safety Method for Risk Evaluation and Assessment

16 December 2024



Contents

1. Introduction	4
Background	4
Where on the railway system does the CSM REA apply?	5
Purpose of this guidance	6
2. Applying the CSM REA	8
When does the CSM REA apply?	8
What are technical, operational and organisational changes?	13
Who has duties under the CSM REA?	14
How does the proposer determine the significance of a change?	15
3. Applying the risk management process of the CSM REA	18
What does the risk management process involve?	18
What are the main phases of the risk management process?	18
Hazard record	31
Other documentation	32
Demonstration of system compliance	32
Independent assessment	33
Avoiding duplication of assessment processes	35
Further information and references	37
4. The role of the assessment body	38
What is the role of the assessment body?	38
Safety assessment report	39
5. Miscellaneous requirements for specific duty holders	41
Railway undertakings and infrastructure managers	41
Entities in charge of maintenance	41
Supervision by national safety authorities	41

Annex A: Determining the significance of a change	42
Annex B: Criteria for assessment bodies	46
Annex C: Guidance on organisational change	48
Annex D: Glossary of terms and acronyms	52
Annex E: Table of updates to guidance	61

1. Introduction

Background

- 1.1 The common safety method (CSM) for risk evaluation and assessment (“the CSM REA”) was established by Commission Implementing Regulation [402/2013](#) and was designed to set out procedures and methods for carrying out risk evaluation and risk control whenever a change in operating conditions to the rail system is being made.
- 1.2 Specifically, the CSM REA establishes a common mandatory risk management process for the rail industry to apply when technical, operational or organisational changes are being made to the rail system that could have an impact on safety. Principally, the CSM REA requires a risk management process to be applied if it is deemed that the changes are significant and could pose a safety risk. The processes are intended to complement requirements in other legislation, for example maintaining a safety management system, and not to duplicate other safety requirements.
- 1.3 The CSM REA, as it applies in the UK, includes amendments made to it by Commission Implementing Regulation (EU) [2015/1136](#) which created harmonised design targets.

Changes resulting from EU Exit

- 1.4 Commission Implementing Regulation 402/2013 was retained and corrected by the Rail Safety (EU Exit) (Amendment etc) Regulations 2019 ([S.I. 2019/837](#)) and the Railways (Safety, Access, Management and Interoperability) (Miscellaneous Amendments and Transitional Provision) (EU Exit) Regulations 2019 ([S.I. 2019/1310](#)) to ensure the CSM REA would continue to be operable in a domestic context following the UK’s withdrawal from the EU and the end of the EU Exit transition period. This guidance document explains the main requirements set out in the retained and corrected version of the CSM REA as it applies to those who have duties under the Railways and Other Guided Transport Systems (Safety) Regulations 2006 (as amended) (SI 2006/599) (“ROGS”). It does not seek to cover all aspects of the ROGS legislation. You may find it helpful to read this guidance document alongside a copy of the ROGS [legislation](#).
- 1.5 The main change to the retained EU legislation relates to the use of relaxed criteria and mutual recognition. While mutual recognition is still permitted between UK assessment bodies, mutual recognition is no longer possible between

assessment bodies recognised in the UK and an EU assessment body. Following EU Exit, a UK proposer no longer has the option to apply relaxed criteria where it does not intend the assessment report to be recognised by another assessment body. All proposers seeking to make a significant change must carry out a risk assessment and appoint an independent assessment body to assess their risk management process.

- 1.6 The retained Commission Implementing Regulation 402/2013 was further amended by the European Union (Future Relationship) Act 2020 ([2020 c.29](#)) to ensure full compliance and consistency with the requirements of the UK-EU Trade and Co-operation Agreement. These amendments were limited to extending the scope of standards that can be designated by the Secretary of State to include technical specifications adopted by international standardising bodies.

Where on the railway system does the CSM REA apply?

- 1.7 The CSM REA has the same scope as the mainline railway as defined in ROGS. Therefore, the CSM REA does not apply to a railway if:

a) ORR determines under regulation 2A (1) of ROGS that it falls within one or more of these categories:

- metros and other light rail systems;
- networks that are functionally separate from the rest of the mainline railway system and intended only for the operation of local, urban or suburban passenger services, as well as transport undertakings operating solely on these networks; or
- heritage, museum or tourist railways that operate on their own networks; or

b) ORR determines under regulation 2A (2) of ROGS that heritage vehicles that operate on the mainline railway and comply with national safety rules are part of a non-mainline operation; or

c) it is privately owned infrastructure that exists solely for use by the infrastructure owner for its own freight operations.

- 1.8 Rail systems that fall under (a) and (b) above are contained in an [Approved list](#) on our website.

- 1.9 The CSM REA primarily applies to Railway Undertakings (RUs), Infrastructure Managers (IMs) and Entities in Charge of Maintenance (ECMs) but also applies to

project entities and manufacturers in certain circumstances (see paragraphs 2.17 - 2.18).

- 1.10 ROGS requires RUs and IMs to develop safety management systems (SMS) to manage the risks associated with their activities and to meet specific criteria. One of the criteria for the SMS is that it must apply the relevant parts of CSMs. In addition to the CSM REA, there is one other CSM applicable to RUs and IMs (the CSM for Monitoring). Please see [ORR's website](#) or [RSSB's Taking Safe Decisions](#) for further details. You will need to be a member of the RSSB to access their guidance. ORR will check compliance with CSMs when we examine applications from duty holders for safety certificates or authorisations and when we subsequently supervise those duty holders.
- 1.11 The Railways and Other Guided Transport Systems (Miscellaneous Amendments) Regulations 2013 ([S.I. 2013/950](#)) removed from ROGS the requirement for a written safety verification scheme by RUs or IMs for non-mainline railways.
- 1.12 The CSM REA does not apply to RUs who operate vehicles within a possession (for example On-Track Machines (OTMs)). If vehicles operate within a possession and subsequently leave the possession to operate on the mainline railway the CSM REA will apply. The risks arising from operating OTMs within a possession can be managed through other measures, such as the Management of Health and Safety at Work Regulations 1999 ([S.I. 1999/3242](#)).
- 1.13 In circumstances where the CSM REA is not a formal legal requirement (for example if the rail system is on the Approved List), the risk management process it describes can nevertheless be used for the management of change.

Purpose of this guidance

- 1.14 This guidance document summarises and explains the main requirements of the CSM REA, to whom it applies, and specific points on compliance in the UK. This includes amendments made by the Rail Safety (Amendment etc.) (EU Exit) Regulations 2019 ([S.I. 2019/837](#)) and the Railways (Safety, Access, Management and Interoperability) (Miscellaneous Amendments and Transitional Provision) (EU Exit) Regulations 2019 ([S.I. 2019/1310](#)) following the UK's withdrawal from the EU.
- 1.15 This guidance will continue to be updated as further revisions to the CSM REA come into force or if there are changes to other related legislation or processes that impact on how the CSM REA should be applied.

1.16 More information can be found at the following:

- [Commission Regulation \(EU\) 402/2013 \(consolidated with Regulation \(EU\) 2015/1136\)](#)
- [Commission Implementing Regulation \(EU\) 2015/1136](#)
- RSSB guidance: Taking Safe Decisions - <http://www.rssb.co.uk/risk-analysis-and-safety-reporting/risk-analysis/taking-safe-decisions>

2. Applying the CSM REA

When does the CSM REA apply?

- 2.1 The starting point for anyone proposing any change in relation to the mainline railway system is the CSM REA. The CSM REA applies when any technical, operational or organisational change is being proposed to the railway system. A person making the change (known as ‘the proposer’) needs to firstly consider if a change has an impact on safety. If there is no impact on safety, the risk management process in the CSM REA does not need to be applied and the proposer must keep a record of how it arrived at its decision.
- 2.2 If the change has an impact on safety the proposer must decide whether it is significant or not by using criteria in the CSM REA (see Annex A of this guidance). If the change is significant the proposer must apply the risk management process (see Chapter 3). If the change is not significant, the proposer is not obliged to apply the risk management process. However, it is strongly recommended that the proposer uses the process to manage non-significant safety risks. The proposer must keep a record of how it arrived at its decision.
- 2.3 This process is summarised in Figure 1 below.
- 2.4 There is other domestic legislation in Great Britain that requires a suitable and sufficient risk assessment to be carried out, such as the Management of Health and Safety at Work Regulations 1999. See paragraph 2.11 for more information. The CSM REA does not replace legal obligations arising from other domestic safety legislation. You should ensure that you understand all legal requirements when undertaking any change on the railway network.

If the change is not significant

- 2.5 In cases where a change is determined not to be significant, it will fall to the proposer of the change to consider domestic legislative requirements, such as those set out in regulation 19 of ROGS and regulation 3 of the Management of Health and Safety at Work Regulations 1999 (“MHSWR”) ([S.I. 1999/3242](#)), which require a suitable and sufficient risk assessment to be undertaken. It is possible to adopt the approach of the risk management process of the CSM REA even when there is no legal requirement to do so (for example, when a change is not significant or if the change relates to non-mainline railway) in line with the organisation’s safety management system. Following the CSM approach correctly

in these circumstances is likely to mean that domestic safety legislation is complied with.

- 2.6 If a non-mainline operator wishes to use CSM REA methodology whilst managing a change under Safety Verification, they must ensure that they still meet the requirements of a Written Safety Verification Scheme within Schedule 4 of ROGS.
- 2.7 The RSSB, in its publication [Taking Safe Decisions](#), recommends applying the risk management process of the CSM REA even if a change is not significant, highlighting that the CSM REA represents good practice for assessing and managing risk.
- 2.8 So, even though it is not mandatory to apply the risk management process if a change is not significant, a proposer may choose to apply it. In these circumstances some elements of the risk management process (such as the need for independent assessment) can be omitted.

If the change is significant

- 2.9 In cases where a change is determined to be significant, the risk management process of the CSM REA must be carried out by the proposer. The framework of the risk management process is based on the analysis and evaluation of hazards using one or more of the following risk acceptance principles:
- application of codes of practice;
 - comparison with similar systems (reference systems); and
 - explicit risk estimation.
- 2.10 Although the risk management process of the CSM REA must always be complied with, it also complements domestic safety legislation. The CSM REA applies the same principles as set out in Regulation 3 of the MHSWR (S.I. 1999/3242) but requires a more formalised process involving an independent evaluation of the risk assessment process by an assessment body (which can be carried out by an in-house service if it meets the criteria in the regulation). The CSM REA also includes additional elements requiring:
- agreements with other duty holders involved in managing or affected by the risk in their risk management process and associated safety management responsibilities; and

- cooperation arrangement between duty holders in how shared risks will be managed.

- 2.11 Duty holders should consider whether any changes being proposed interface with other legislation, such as MHSWR and the Construction (Design and Management) Regulations 2007 ([S.I. 2007/320](#)) (“the CDM Regulation”) which also require the proposer to assess safety risk. Whilst it is possible to carry out separate risk assessments under each piece of legislation, in these cases it is likely to be more efficient to produce a single, broadly scoped, risk assessment in accordance with the CSM REA that addresses the risks for the whole operation as a result of the proposed change. The scope of the risk management process should be recorded in the System Definition.
- 2.12 Conflict should not arise between separate domestic legislative provisions in relation to risk assessments. The CSM REA, ROGS, MHSWR and CDM Regulation requirements seek to achieve the same result: a robust risk assessment and controls to maintain or reduce risk. ORR therefore considers it to be unnecessary for duty holders to produce separate risk assessment and evaluation processes to comply with domestic requirements. Compliance with the CSM REA should simultaneously deliver compliance with regulation 19 ROGS and regulation 3 MHSWR in respect of the change and impact on other interfaces, as the purpose of the CSM REA is to deliver a thorough and competent risk assessment process.
- 2.13 Significantly, a court is likely to interpret legislation in such a way as to determine that a risk assessment which is CSM REA compliant is suitable and sufficient to meet domestic requirements.
- 2.14 If a proposer of a change applies one or more of the three risk acceptance principles in the CSM REA regulation correctly for all identified hazards, and implements suitable control measures, this should mean that the risk has been reduced to an acceptable level for the change being carried out. One of the purposes of the CSM REA is to ensure that a high level of safety will be maintained and, where reasonably practicable, improved.

Designing in risk control

- 2.15 It is essential that duty holders’ risk assessment and evaluation processes consider risk control from the initial design stage. Where the change is likely to be significant this will require the CSM REA to be considered early enough in the process to influence the client requirements before pre-construction information is finalised.

Other duties

2.16 Duty holders need to comply with all relevant health and safety obligations as part of their railway activities, such as the Management of Health and Safety at Work Regulations 1999 ([S.I. 1999/3242](#)), the Railway Safety (Miscellaneous Provisions) Regulations 1997 ([S.I. 1997/553](#)) and the Railway Safety Regulations 1999 ([S.I. 1999/2244](#)). You should ensure that you understand all your legal requirements when undertaking any change on the railway network.

Further instances where the CSM REA may be required

2.17 In addition to technical, operational or organisational changes, application of the CSM REA may be required:

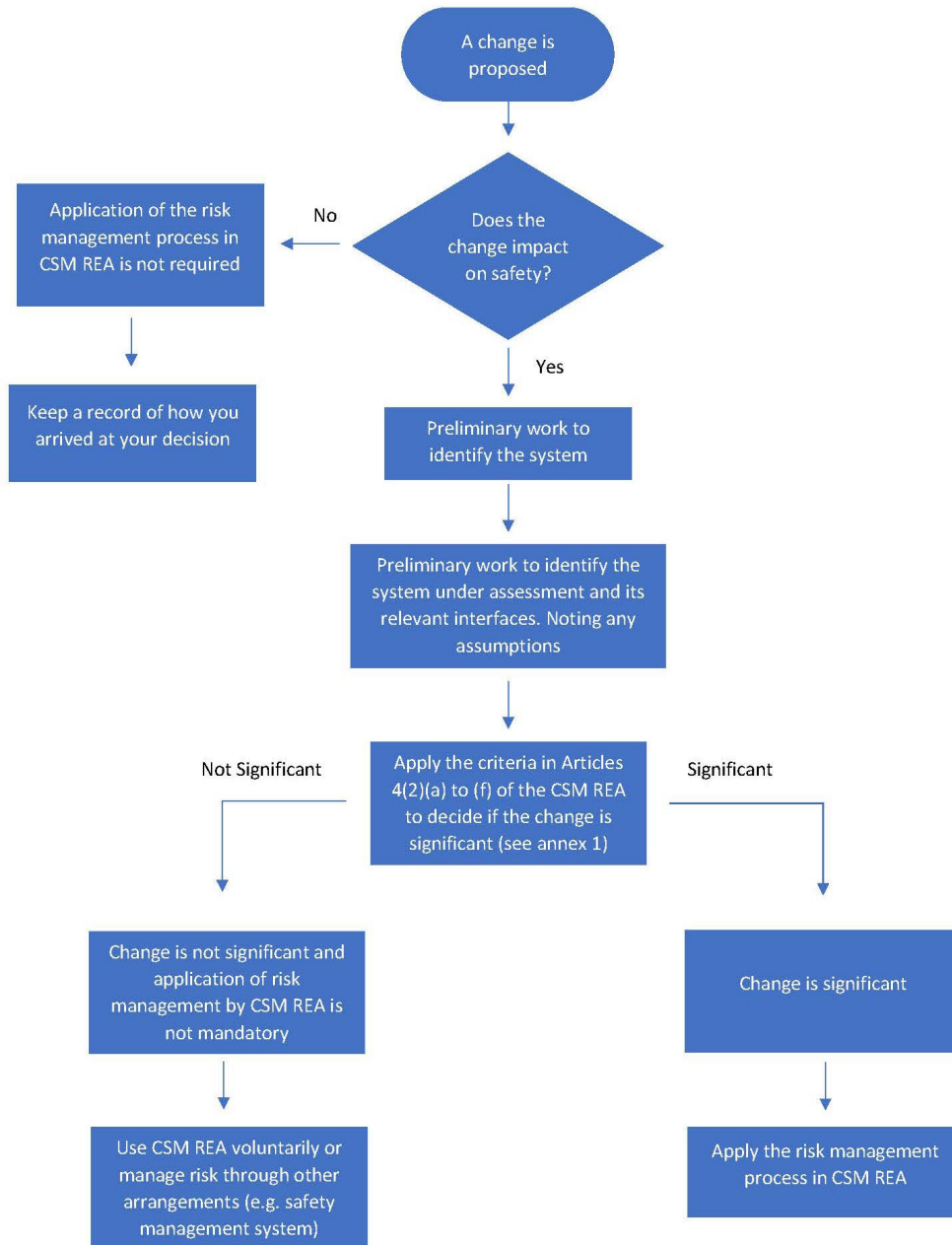
- by a National Technical Specification Notice (NTSN) when structural subsystems falling within the scope of the Railways (Interoperability) Regulations 2011 (as amended) (RIR) ([S.I. 2011/3066](#)) are constructed or manufactured, or upgraded or renewed; or
- when placing in service a structural subsystem to ensure that it is integrated into the existing system in a safe manner.

2.18 UK railway technical standards, known as National Technical Specification Notices (NTSNs) replaced EU technical specifications for interoperability (TSIs) in Great Britain on 1 January 2021 (TSIs continue to apply in Northern Ireland). They set standards to be complied with in relation to the design, construction, placing in service, upgrading, renewal, operation and maintenance of the parts of the mainline rail system, as well as the professional qualifications and health and safety conditions of the staff who contribute to its operation and maintenance. For further information, see [here](#).

2.19 Structural subsystems (as described in Schedule III of the Railways (Interoperability) Regulations 2011 ([S.I. 2011/3066](#)), as amended by the Railways (Interoperability) (Amendment) (EU Exit) Regulations 2019) ([S.I. 2019/345](#)) are:

- rolling stock;
- infrastructure;
- control, command and signalling; and
- energy.

Figure 1 – Applying the CSM REA for technical, operational and organisational change



What are technical, operational and organisational changes?

Technical changes

2.20 Technical changes are changes to a structural subsystem such as new rolling stock or a station rebuild. Technical changes should also be reviewed to determine whether they introduce changes to the operation of the subsystem under consideration.

Operational changes

2.21 Operational changes are:

- changes to the operation of a structural subsystem;
- changes to the operation of the railway system; or
- changes to the operating rules of the railway system.

2.22 Operational changes are often the result of technical changes to a subsystem. Indeed, technical changes are frequently made for the purpose of delivering a desired operational change. In these cases, the technical change and its effect on:

- the operation of the subsystem;
- the wider railway system; or
- the operating rules of the railway, must be considered and assessed together.

2.23 For example, a change of the control, command and signalling (CCS) system from fixed marker signals (for example TVM) to a cab-based system (for example ETCS) is a significant safety-related technical change that should be assessed in accordance with the risk management process of the CSM REA. Such a change will also involve changes to the operation of the CCS sub-system and changes to the wider operating rules. These operational changes must be assessed together with the significant safety-related technical changes as part of the risk management process of the CSM REA.

2.24 Of course, changes to:

- the operation of a sub-system; or

- the operation of the railway system; or
- the operating rules of the railway system

can also be introduced without a related technical change. If these changes are safety-related, the proposer should consider whether they are significant or not. Only if they are significant should the risk management process of the CSM REA be applied to them. If the change is not significant, the proposer must keep a record of how it arrived at its decision.

Organisational changes

- 2.25 Organisational changes are changes to the organisation of a duty holder in the railway system which could impact on the safety of the railway system. In most cases, this is likely to mean changes to an IM or an RU, but it could be an ECM or any other organisation that affects the safety of the railway system.
- 2.26 An example could be a change to the Safety Management System (SMS) - moving from a structure and culture, based on a large number of prescriptive standards, to a risk-based system relying on trained and competent staff using a small number of key principles. This could be a significant safety-related change and should be assessed using the CSM REA.
- 2.27 Further guidance on organisational changes can be found in Annex C.

Who has duties under the CSM REA?

- 2.28 The CSM REA places duties primarily on the proposer of a change. Proposers are those in charge of projects who wish to implement a change to a technical, operational or organisational aspect of the railway system.
- 2.29 In many circumstances, proposers will be RUs or IMs. An ECM will also become a proposer in relation to changes to its maintenance system, or if it is responsible for the modification of vehicles.
- 2.30 However, the CSM REA allows other bodies to act as the proposer. This could apply, for example, to project entities and manufacturers who lead projects where they are required to engage an Approved Body (ApBo) or a Designated Body (DeBo), or an applicant for an authorisation for placing in service under RIR.
- 2.31 In some circumstances a manufacturer or client will act as the proposer at the start of a project, for example if they want to market a new or altered product and/or there is no RU or IM in place. For manufacturers, once the product is placed on

the market, that 'change' is complete and an RU or IM wishing to use the new or altered product in a specific application or location will then be the proposer of a new change for CSM REA purposes. The RU or IM's risk assessment will focus on such matters as route-specific technical compatibility and safe integration and will not need to repeat the manufacturer's risk assessment. In projects where a client is undertaking the initial design and development work the client will carry out the obligations under CSM REA initially and once an RU or IM is appointed, the RU and/or IM will then take on the outcomes of the client's initial CSM REA work and incorporate that into their ongoing CSM REA duties.

- 2.32 It may be advisable to ensure that the obligations on the manufacturer/client to apply CSM REA, in particular the requirement to appoint an independent Assessment Body (see chapter 4), before handing the product/project over to the RU/IM is included in the commercial contractual arrangements between the two parties.
- 2.33 The proposer must ensure that risks introduced by its suppliers and its service providers, including their subcontractors, are also managed through application of the CSM REA. This may require participation in the risk management process of the CSM REA through contractual arrangements coordinated by the proposer.

How does the proposer determine the significance of a change?

- 2.34 If a proposed change has an impact on safety, the proposer must determine the significance of the change by examining the criteria in Article 4(2) of the CSM REA (see Annex A of this guidance). Note that the assessment body (see Chapter 4) assesses the application of the risk management process of the CSM REA but cannot question the proposer's significance decision.
- 2.35 If a change is deemed to be non-significant, application of the risk management process of the CSM REA is not mandatory and the change should be managed under the change management processes as described in the proposer's SMS or by carrying out a risk assessment which is required as part of compliance with other legislation, such as the Management of Health and Safety at Work Regulations 1999 (S.I. 1999/3242). However, there is nothing to prevent the proposer voluntarily applying the CSM REA risk management process for a non-significant change.

2.36 ORR may check the process that RUs or IMs have used to determine whether or not to apply the CSM REA. Proposers, therefore, must document their decisions, particularly in relation to the test for significance.

2.37 The CSM REA contains six criteria which should be examined to determine 'significance'. These are:

- **failure consequence:** credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;
- **novelty used in implementing the change:** this concerns both what is innovative in the railway sector, and what is new just for the organisation implementing the change;
- **complexity of the change;**
- **monitoring:** the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;
- **reversibility:** the inability to revert to the system before the change; and
- **additionality:** assessment of the significance of the change, taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.

2.38 The CSM REA gives no order or priority on how to use the "significance" criteria, nor any thresholds to evaluate and make the decision.

Additionality

2.39 Additionality can be described as considering other changes that have been made since the entry into force of the CSM REA (23 May 2013) or since the last application of the risk management process (whichever is later) which, when combined with the change being considered, could become significant. If there are other safety-related changes that have been made 'recently', the test for significance should be made for all the changes as a whole, rather than for just the individual change being considered.

2.40 Annex A suggests that additionality should be considered first as this defines the scope of the change that is to be assessed. It also proposes a method of addressing how far back to look when examining a series of changes.

- 2.41 Breaking down a significant change into a series of smaller changes - which individually are not significant - so that the risk management process is then not applied to the overall significant change is not permitted by the CSM REA.

Novelty and complexity

- 2.42 If a proposed change is novel or complex there could be an increase in the likelihood that, once implemented, the changed structural sub-system, operation or organisation will not behave as predicted and that unforeseen hazards will arise. Classifying such changes as significant and applying the risk management process, including the requirement for an independent assessment, will provide additional assurance and should help to identify measures to mitigate any potential increase in the risk.

3. Applying the risk management process of the CSM REA

What does the risk management process involve?

- 3.1 The risk management process is contained in Annex I of the CSM REA. The main phases are illustrated in Figure 2 and further details are set out below. The process illustrated is not static or linear as the proposer may undertake iterations of all or part of the process. The proposer should also integrate the process into the project lifecycle, rather than carrying it out in isolation. The process begins with a system definition and ends when the proposer is content that for each hazard the identified safety requirements and measures have been complied with by applying defined risk acceptance principles (see paragraph 3.25). If the proposer decides to change the system definition throughout the process, it may need to start again from the beginning.
- 3.2 An assessment body must carry out an independent assessment of the risk management process and the results obtained from carrying it out.
- 3.3 The processes required by Annex I of the CSM REA will be familiar to many in the UK and are probably already in use in their risk management systems. The key requirements are examined below. Potential proposers who need to comply with the risk management process should review their current processes and procedures and make any necessary adjustments.

What are the main phases of the risk management process?

Preliminary system definition

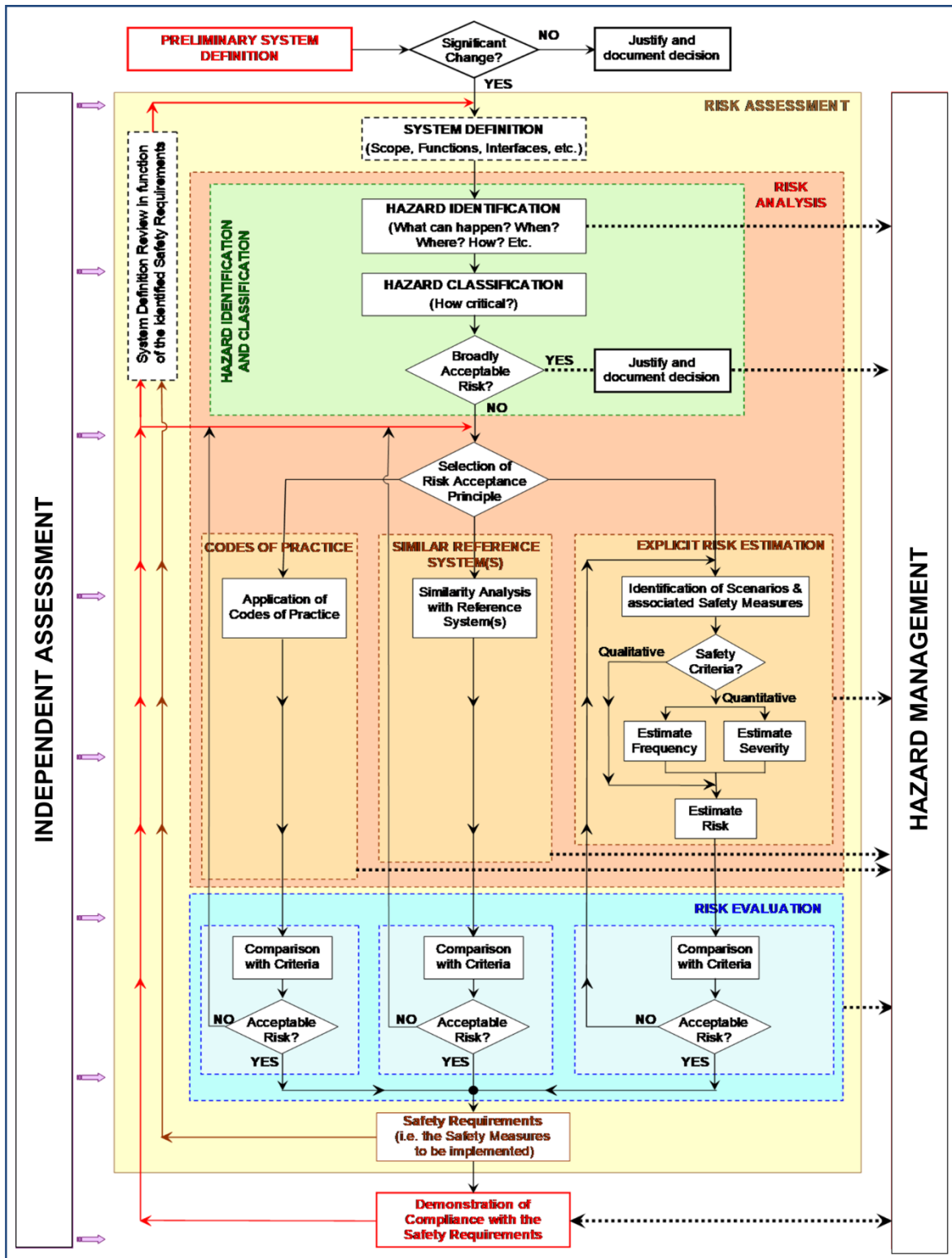
- 3.4 In order to assess whether the change is significant or not, the proposer should conduct a preliminary system definition. This 'preliminary system definition' is in effect an analysis of what is being changed and a preliminary risk assessment of that change. The 'preliminary system definition' should:
- give a clear statement on what is being changed and the scope of the change; and

- address the information described in paragraph 3.9 (a) to (d) to the extent necessary to enable the proposer to determine the significance of the change.

System definition

3.5 The risk assessment process starts with the system definition (which can use information from the preliminary system definition). This provides the key details of the system that is being changed - its purpose, functions, interfaces and the existing safety measures that apply to it. In most cases, the hazards which need to be analysed will exist at the boundary of the system with its environment.

Figure 2: Risk management process and independent assessment



3.6 The definition is not static and during iterations of the risk management process, it should be reviewed and updated with the additional safety requirements that are identified by the risk analysis. It therefore describes the condition (or expected condition) of the system before the change, during the change and after the change.

3.7 The system definition may change due to factors other than the specification of safety requirements, such as:

- changes in scope;
- changes in client requirements;
- increasing design definition; and
- implementation of changes proposed by contractors and suppliers.

3.8 Such changes may necessitate iteration of the risk management process.

Equally, changes to the system definition for other reasons may require the proposer to repeat all or part of the process and discuss with the assessment body the implications.

3.9 The risk management process states that the system definition should address at least the following issues:

- a) system objective, e.g. intended purpose;
- b) system functions and elements, where relevant (including e.g. human, technical and operational elements);
- c) system boundary including other interacting systems;
- d) physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces;
- e) system environment (e.g. energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use);
- f) existing safety measures and, after iterations, definition of the safety requirements identified by the risk assessment process; and
- g) assumptions which shall determine the limits for the risk assessment.

- 3.10 The system definition needs to cover not only normal mode operations but also degraded or emergency mode.
- 3.11 Consideration of interfaces should not be restricted to physical parameters, such as interfaces between wheel and rail. It should include human interfaces, such as the user-machine interface between the driver and driver displays in the cabs of rail vehicles. It should also include interfaces with non-railway installations and organisations. For example, the interface with road users at level crossings.
- 3.12 Operational rules and procedures, and staff competence should be considered as part of the system environment. This is in addition to the more usual issues such as weather, electromagnetic interference, local conditions such as lighting levels, etc.
- 3.13 A good test of whether the system definition is complete and sufficient is if the proposer can describe the system elements, boundaries and interfaces, as well as what the system does.
- 3.14 The description can effectively serve as a model of the system and should cover:
- structural issues (how the system is constructed or made up); and
 - operational issues (what it does, and how it behaves normally and in failure modes).
- 3.15 The existing safety measures, which may change as the risk assessment process progresses, can be added after the structural and operational parts of the model are complete.
- 3.16 For some projects, the proposer may not know all the environmental or operational conditions in which the altered or new system will operate. In these circumstances, they should make assumptions on the basis of the intended or most likely environment. These assumptions will determine the initial limits of use of the system and should be recorded. When the system is put into use, the proposer (who may be different to the original proposer) should review the assumptions and analyse any differences with the intended environmental and operational conditions.

Hazard Identification

- 3.17 The purpose of the hazard identification is to identify all reasonably foreseeable hazards which are then analysed further in the next steps.

- 3.18 The hazard identification should be systematic and structured, which means taking into account factors such as:
- the boundary of the system and its interactions with the environment;
 - the system's modes of operation (i.e. normal/degraded/emergency);
 - the system life cycle including maintenance;
 - the circumstances of operation (e.g. freight-only line, tunnel, bridge, etc.);
 - human factors;
 - environmental conditions; and
 - relevant and foreseeable system failure modes.
- 3.19 While the risk management process does not require that any specific tools should be applied, many of the more well-known techniques will be relevant, including
- structured group discussions;
 - checklists;
 - task analysis;
 - hazard and operability studies (HAZOPs);
 - hazard identification studies (HAZIDs);
 - failure mode and effects analysis (FMEA);
 - fault trees; and
 - event trees.
- 3.20 Whichever technique is used, it is important to have the right mixture of experience and competence while maintaining impartiality and objectivity. Correct hazard identification will underpin the whole risk management process and give assurance that the risks will be managed in the project.
- 3.21 The risk management process uses the term 'broadly acceptable' to identify those hazards which need not be analysed further. In this context, 'broadly acceptable' applies to those hazards where the risk is, to all intents and purposes, insignificant or negligible. This could be because the hazard is so unlikely to arise that there

are no feasible control measures that could be used to control the risk it creates or where there is a credible failure mode, but the consequences are negligible. An example of a very low frequency, very high severity event is a 'meteorite impact'; and an example of a high frequency, very low severity event is a 'paper cut'. By screening out the 'broadly acceptable' hazards at this stage, the risk analysis can focus on the more important hazards to manage. It is unlikely that many hazards will be screened out in this way.

- 3.22 The level of detail of the hazard identification depends on the system that is being assessed and needs to be sufficient to ensure that relevant safety measures can be identified. If, following a high-level hazard identification, it can be successfully demonstrated that the hazard can be controlled by application of one of the three risk acceptance principles required by the risk management process (see paragraph 3.25), then no further hazard identification is necessary unless it is required as part of the application of the explicit risk estimation principle. If it is not possible to have sufficient confidence at this stage, then the high-level hazard may be broken down into its component parts allowing further analysis of the causes and consequences and identification of relevant measures to control the risks arising. The risk management risk framework (see [Reducing Risks: Protecting People](#)) process continues until it can be shown that the overall system risk is controlled by one or more of the risk acceptance principles.
- 3.23 Hazard identification is still necessary for those changes where the hazards are to be controlled by the application of codes of practice or by comparison to reference systems. Hazard identification in these cases will serve to check that all the identified hazards are being controlled by relevant codes of practice or by adopting the safety measures for an appropriate in-use system. The hazard identification can then be limited to verification of the relevance of the codes of practice or reference systems, if these completely control the hazards, and identification of any deviations from them. If there are no deviations, the hazard identification may be considered complete.
- 3.24 The purpose of risk analyses and evaluation is to identify those safety requirements and measures that are necessary to control the risks arising from the identified hazards.

Risk acceptance principles

- 3.25 Hazards can be analysed and evaluated using one or more of the following risk acceptance principles:
- the application of codes of practice;

- a comparison with similar systems (reference systems); or
- an explicit risk estimation.

3.26 In the UK, you can choose any of these three risk acceptance principles.

3.27 Individual hazards can be closed out by the application of one or more of the three principles. However, it is likely that different principles will be used for different hazards. Any risk assessment conducted under the CSM REA should always be proportionate to the extent of the risk being assessed.

3.28 The CSM REA has been introduced to ensure that levels of safety are maintained or improved when and where necessary and reasonably practicable, in accordance with the requirements of the Railway Safety Directive (2004/49/EC). Applying one or more of the three risk acceptance principles correctly for all identified hazards and implementing suitable control measures should mean that the risk acceptance criteria (see 3.48) has been met. In these circumstances, ORR will not normally require further evidence that the residual risk is acceptable.

Codes of Practice

3.29 Standards and rules must meet all the following criteria to be used as a code of practice for the risk management process:

- be widely accepted in the railway sector or otherwise justified to the assessment body;
- be relevant for the control of the specific hazard; and
- be available to an assessment body so that it can:
 - (ii) assess the suitability of how the CSM REA is applied and the results of applying it; or
 - (iii) mutually recognise any safety assessment report on the same system within the UK (see paragraph 4.8).

3.30 Standards and rules that are widely accepted in the railway sector include:

- National Technical Specification Notices (NTSNs);
- National technical rules (NTRs); and
- Euro standards or ISO standards.

3.31 Domestic or UK standards can also be used where they meet the requirements in paragraph 3.29 and are not in conflict with mandatory standards. In particular, Railway Group Standards (RGS) and Rail Industry Standards (RIS) are widely acknowledged in the UK railway industry. There are a number of other domestic standards that are available to all railway duty holders that could be considered as codes of practice in certain circumstances, such as:

- Rail Industry Company Standards;
- codes of practice relating to plant produced by the Mechanical and Electrical Engineers Networking Group for the rail industry; or
- relevant British Standards issued by the [British Standards Institution](#); or
- other rail industry standards.

This list is not exhaustive.

3.32 While there is no mandatory fire safety standard within the framework of technical standards, and fire safety is not directly referenced in railway safety legislation, fire safety is an important issue and should be considered with any risk assessment when changes are being proposed to a system. Proposers making any changes to the railway should identify any appropriate fire safety standards for their work (i.e. in codes of practice), or alternative situation-specific means of managing risks, by applying the CSM REA.

3.33 It is also possible to use standards or codes of practice from other sectors, for example aviation and maritime, but these must be justified and be acceptable to the assessment body (see paragraphs 3.66 - 3.82). The proposer will have to demonstrate that they are effective in controlling the risks from the relevant hazards in a railway context.

3.34 To be satisfied that a code of practice is relevant for the control of the specific hazards in the system, the proposer needs to:

- know what the hazards are;
- be able to demonstrate that the code(s) of practice are relevant to the hazards; and
- be able to demonstrate that application of the code(s) of practice control the hazards.

- 3.35 In evaluating whether a code of practice controls one or more of the hazards, proposers will need to check, with the support of other affected parties, that it covers the intended application of the system under assessment.
- 3.36 Deviations from codes of practice are possible where the proposer can demonstrate that at least the same level of safety will be achieved. Mandatory standards such as NTSNs and RGSs include a process for deviating from them.
- 3.37 Most non-mandatory standards do not have a process for deviating from them. If one or more conditions of the code of practice are not fulfilled but there are residual hazards in the system under assessment that the code of practice is relevant to, the proposer may have to conduct an explicit risk estimation on those hazards. Alternatively, other codes of practice or reference systems could be used.

Reference systems

- 3.38 Reference systems can be used to derive the safety requirements for the new or changed system. For an existing system to be used as a reference system, a proposer needs to demonstrate that as a minimum:
- it has already been proven in use to have an acceptable safety level and would therefore still qualify for approval; and
 - the system being assessed is used under similar functional, operational and environmental conditions and has similar interfaces as the reference system.
- 3.39 For technical changes, it is unlikely that evidence of in-service history alone can prove that a high integrity system has an acceptable safety level, given the low failure rates required of such systems. Evidence that sufficient safety engineering principles have been applied in the development of the reference system will need to be confirmed for each new application. Therefore, when a technical system under assessment is compared with a similar reference system, the new technical system under assessment must comply with the same safety requirements of the old one since they are both used to demonstrate the acceptance of the risk associated with the reference system. 'Safety requirements' include:
- the redundancy of the architecture used for the reference system;
 - the engineering principles; and
 - the application of safety and quality processes commensurate with the safety integrity level expected for the technical system under assessment.

Proven in use to have an acceptable safety level

- 3.40 There needs to be robust monitoring of the return of experience of the reference system to demonstrate that it has been 'proven in use to have an acceptable safety level'. This is the 'risk monitoring' part of the risk management process. It aims to check that the failure rate actually achieved by the reference system is not worse than the value used during the predictive risk assessment. It is therefore necessary to monitor the achieved failure occurrence of the reference system and verify that, when failed, the reference system is not in an unsafe state. The number of 'unsafe' failure occurrences; the number of items of the reference system already in use; and the number of operating hours per day are all needed to determine the failure rate achieved by the reference system.
- 3.41 The proposer must use the support of other affected parties to analyse whether one; several; or all hazards are appropriately covered by a similar reference system. If the reference system meets the requirements in paragraph 3.40, and those in paragraph 3.39 for technical changes, the hazards and associated risks covered by that system are considered as acceptable. If there are deviations, the safety requirements can still be used for the hazards that are covered by the reference system, providing the same level of performance can be demonstrated. This may involve further risk assessment and evaluation. If the same performance or better cannot be reached, additional safety measures need to be identified by applying one of the other two risk acceptance principles.

Explicit risk estimation

- 3.42 Explicit risk estimation is an assessment of the risks associated with hazard(s), where risk is defined as a combination of the rate of the occurrence of the hazard or hazardous event causing harm (the frequency) and the degree of severity of the harm (the consequence).
- 3.43 The estimation can be qualitative, quantitative or a combination of the two. The choice will be determined by factors such as the availability of quantitative data and confidence in such data. Any analysis should be proportionate to the potential risks. Any risk assessment should follow a systematic and structured process.
- 3.44 A typical risk assessment process in the UK rail industry for the type of projects that are likely to be significant would be:
- identifying the hazardous events which have the potential to cause injury or death to:
 - passengers;

- workers; or
- members of the public who are directly or indirectly exposed to the technical, operational, or organisational change being assessed;
- identifying the precursors (i.e. the component, sub-system or system failures, physical effects, human error failures or operational conditions), which can result in the occurrence of each hazardous event;
- identifying the control measures that are in place to control or limit the occurrence of each precursor that cannot be eliminated;
- estimating the frequency at which each precursor and hazardous event can occur;
- estimating or analysing the consequences in terms of injuries and fatalities that could occur for the different outcomes that may follow the occurrence of a hazardous event;
- estimating the overall risk associated with each hazardous event;
- identifying any additional control measures required to ensure that risk is reduced so far as is reasonably practicable; and
- providing clear and comprehensive documentary evidence of the methodologies, assumptions, data, judgements and interpretations used in the development of the risk assessment and the analysis of its results (The results may also need to be accompanied by sensitivity and uncertainty analyses, particularly where the assessment is quantitative and where different safety measures need to be evaluated).

3.45 Explicit risk estimation can be used where:

- a proposer is unable to address the hazards identified in the hazard identification stage of the risk management process via a code of practice or comparison with a reference system;
- deviations are necessary from codes of practice or reference systems; or
- a proposer needs to analyse the hazards and evaluate design principles or safety measures.

3.46 The CSM REA does not impose any specific tools and techniques to be used in an explicit risk estimation but:

- The methods used must correctly reflect the system under assessment and its parameters (including all operational modes); and
- The results obtained must be sufficiently accurate to provide a robust basis for decision-making (minor changes in input assumptions or prerequisites must not result in significantly different requirements).

3.47 Proposers may find the [Guidance on the Common Safety Method for Risk Evaluation and Assessment](#) (GE/GN 8646) useful for explicit risk estimation.

Risk acceptance criteria for explicit risk estimation

3.48 Risk acceptance criteria are used to judge whether the risk is sufficiently reduced to allow the proposer to accept and implement the change. Depending on the risk acceptance criteria, the proposer can evaluate the acceptability of the risk for each associated hazard either individually or collectively. If the estimated risk is not acceptable, the proposer must identify and implement additional safety measures to reduce the risk to an acceptable level. For the UK, this will mean that risks should be reduced 'so far as is reasonably practicable' (see [ORR SFAIRP guidance](#)).

Harmonised design targets

3.49 Where hazards arise as a result of failures of functions of an Electrical, Electronic and Programmable Electronic technical system (E/E/PE) (see paragraph 3.50 for further description of an applicable technical system) and the proposer decides to perform quantitative risk assessment in the scope of application of the explicit risk estimation risk acceptance principle, harmonised design targets shall apply to those failures as follows:

- (a) In cases where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable (i.e. an occurrence of failure at a frequency less than or equal to 10^{-9} per operating hour).
- (b) In cases where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be

improbable (i.e. an occurrence of failure at a frequency less than or equal to 10^{-7} per operating hour).

- 3.50 The harmonised design targets set out in 3.49 above are applicable for the design of E/E/PE technical systems. The design targets cannot be used for: the design of purely mechanical technical systems, providing overall quantitative targets for the whole railway system, and controlling hazards arising from the purely mechanical part of a technical system.

Catastrophic accident

- 3.51 A catastrophic accident is one that typically affects a large number of people and results in multiple fatalities.

Critical accident

- 3.52 A critical accident is one that typically affects a very small number of people and results in at least one fatality.

Hazard record

- 3.53 The proposer has to create and maintain a hazard record for the system (or part system) that is to be changed. Its purpose is to track progress of the risk assessment and risk management process for the project. The CSM REA requires that it contains certain information but does not mandate any particular format.
- 3.54 The hazard record should concentrate on key issues. To aid transparency and consistency, it needs to contain the safety measures relating to the identified hazards and the assumptions taken into account in the definition of the system. It needs to include details of the risk assessment principles used and the duty holders in charge of controlling each hazard.
- 3.55 When the change has been 'accepted' by the proposer, and is successfully embedded in the system, the hazard record should be integrated by the IM or RU operating the system into its SMS. This may be examined by the ORR as part of its inspection of a duty holder's SMS.
- 3.56 The hazard record itself should be updated if:
- other significant changes occur that affect the system;
 - a new hazard is discovered;
 - there are new accident and incident data; or

- assumptions about the system are changed.

3.57 The hazard record, if kept updated, may also be of value where the system is later used as a reference system.

3.58 There may be more than one hazard record if there are several bodies participating in the change. If separate hazard records are maintained during the project, the proposer is responsible for co-ordinating the production of an overall record.

Other documentation

3.59 The CSM REA places some minimum requirements on proposers to document certain information to assist the assessment body. These are:

- a description of the organisation and the experts appointed to carry out the risk assessment process;
- the results of the different phases of the risk assessment and a list of all the necessary safety requirements to be fulfilled in order to control the risk to an acceptable level;
- evidence of compliance with all the necessary safety requirements; and
- all assumptions relevant for system integration, operation or maintenance, which were made during system definition, design and risk assessment.

Demonstration of system compliance

3.60 The proposer 'accepts' the change in the system and is responsible for its safe integration and operation in the wider railway system. This means ensuring that the system is designed, validated and accepted against the safety measures identified to control the hazards. Before acceptance, the proposer needs to demonstrate that the risk assessment principles have been correctly applied and that the system complies with all specified requirements. The proposer has overall responsibility for coordinating and managing the demonstration that the safety requirements are met. Other organisations involved will need to demonstrate that they have met the safety requirements and implemented safety measures at the lower level for the part of the system for which they are responsible.

3.61 The proposer allocates the safety requirements to each part of the system that was defined in the system definition, but these can also be transferred to other

organisations. If that happens, it should be recorded as such in the hazard record. Contracts may be required to reflect these agreements.

- 3.62 Many hazards, and the risks arising, will be at shared interfaces and cooperation will be needed to ensure that such risks are properly assessed and controlled.
- 3.63 The demonstration of compliance can involve further activities including causal analyses, testing, etc. It is also possible that new hazards may be identified during the validation phase which will need to be analysed further. Where a non-compliance with safety requirements is discovered, then the proposer must be notified. The proposer must then further notify others who are affected and responsible for the same or similar sub-systems so that they can take the appropriate action.

Independent assessment

- 3.64 The CSM REA requires an independent assessment of:
- how the risk management process is applied; and
 - the results from the risk management process.
- 3.65 An assessment body must carry out the independent assessment.
- 3.66 The proposer is able to choose (subject to certain restrictions) the assessment body.
- 3.67 The proposer is required to appoint an assessment body at the earliest appropriate stage of the risk assessment process. However, ORR recommends that the assessment body is involved from the beginning of the project so that it can monitor the development of the hazard record, consider other relevant material (such as a safety plan) and possibly ask to observe tests. This may also include the detailed design stage or the manufacturing stage of the project.
- 3.68 The assessment body must ensure that it has a thorough understanding of the significant change taking place, based on the documentation provided by the proposer. The assessment body should conduct an assessment of the processes used for managing safety and quality during the design and implementation of the significant change, together with an assessment of the application of those safety and quality processes during the design and implementation of the significant change.

- 3.69 The proposer no longer has the option to apply relaxed criteria if it did not intend for the assessment report to be recognised by another assessment body. As a result, all proposers seeking to make a significant change must appoint an assessment body to carry out an independent assessment of the suitability of both the application of the risk management process and of its results.
- 3.70 The proposer can appoint an assessment body external to the organisation or an in-house assessment body. Factors that enable the proposer to demonstrate that an in-house assessment body is independent include:
- Different line management;
 - No involvement with the development of the safety measures associated with the system under assessment; and
 - Freedom from undue commercial influence or bias.
- 3.71 The assessment body can be made up of more than one organisation.
- 3.72 The scale and complexity of any given project may determine whether an external or in-house assessment body is used. For more complex projects, or those where the proposer is unfamiliar with the technical analytical skills needed for the assessment, access to external independent assessment may be needed.
- 3.73 The process for taking the decision about use of internal or external assessment bodies should be recorded. Relevant factors include:
- evidence to satisfy the proposer that the assessment body is independent and competent;
 - absence of financial pressure or incentives on the assessment body (noting that the proposer cannot control financial pressure or incentives from third parties);
 - checks that the assessment body has suitable liability insurance, if it is an external organisation; and
 - appropriate policies relating to confidentiality rules, if the assessment body is an external organisation.
- 3.74 ISO/IEC 17020:2012 specifies the requirements for the competence of bodies performing inspections and for the impartiality and consistency of their inspection activities. It applies to inspection bodies of type A, B or C, as defined in ISO/IEC

17020:2012, and it applies to any stage of inspection. The categorisation of inspection bodies as type A, B or C is a measure of their independence and determines the conditions under which it performs its services.

- 3.75 The accreditation type that an inspection body receives is independent from the requirements under the CSM-REA. Under Article 6 of CSM-REA, AsBos carrying out an independent assessment of the suitability of the application of the risk management process must meet the criteria for accreditation under ISO/IEC 17020:2012. Any type of inspection body, regardless of whether it is type A, type B or type C, can be appointed as an AsBo for the purposes of undertaking an independent assessment provided it meets these requirements.
- 3.76 At the conclusion of the independent assessment, the assessment body produces a safety assessment report, and this should facilitate the proposer's review of the management of the safety system. If the proposer disagrees with any part of the safety assessment report it must keep a record of this with clear justification for its disagreement.

Declaration by the proposer

- 3.77 When the proposer receives the safety assessment report at the end of the risk management process it must produce a written declaration confirming that all identified hazards and associated risks are controlled to an acceptable level.
- 3.78 If the change to the system requires an authorisation for placing in service, the proposer's declaration will be accepted by the:
- ApBo when delivering a conformity certificate (unless it justifies and documents its doubts about the assumptions made or the appropriateness of the results from the assessment); and
 - ORR in its authorisation decision (unless it can demonstrate the existence of a substantial safety risk).
- 3.79 If the change to the system does not require an authorisation for placing in service, then the proposer's declaration must be kept as part of its records.

Avoiding duplication of assessment processes

- 3.80 There are a number of assessment processes required under different laws:
- assessment of conformity with NTSNs (by an ApBo);

- assessment of conformity with NTRs (by a DeBo);
- assessment of safety certificates for RUs (by ORR);
- assessment of safety authorisations for IMs (by ORR);
- independent assessment under the CSM (by an assessment body); and
- assessment of the system of maintenance of ECMs (by a certification body).

3.81 ORR's position is that there should not be duplication when these processes are carried out, and there are opportunities for businesses to avoid duplication by being aware of the following points:

- An ApBo can act as an assessment body as long as it meets the criteria in the CSM REA. So, if the significant change concerns sub-systems that are covered by NTSNs, it is possible to appoint an ApBo that meets the criteria for independent assessment so that it can carry out the CSM assessment as well as the assessment of conformity with NTSNs. Similarly, it is possible to appoint a DeBo that meets the criteria for independent assessment so that it might carry out the CSM assessment as well as the assessment of conformity of NTRs.
- If ORR has issued a safety certificate or authorisation, then the assessment body does not need to examine the general processes for risk assessment during the application of the CSM REA. However, the assessment body should look at how the processes are applied for the specific change. If the assessment body finds that there are issues with the general processes for risk assessment these should be reported to ORR and the proposer.
- If the proposer does not have a safety certificate, safety authorisation, or ECM certificate, then quality management systems may give the assessment body assurance about the general processes for change management and risk assessment within the proposer's organisation.
- If the proposer does not have a safety certificate or safety authorisation, the proposer should, as far as possible, apply equivalent change management and risk assessment processes to those of the duty holder (IM or RU) who is likely to introduce that significant change onto the railway system.

3.82 The CSM REA allows, but does not oblige, National Safety Authorities to act as an independent assessment body when a significant change also concerns:

- an authorisation for placing a structural sub-system or vehicle into service; or
- an update or revision of a safety certificate or safety authorisation.

3.83 ORR does not intend to act as an assessment body in these circumstances.

Further information and references

ORR guidance

3.84 ORR guidance on assessing whether risks on Britain's railways have been reduced so far as is reasonably practicable:

[ORR SFAIRP guidance](#)

Industry guidance

RSSB guidance: Taking Safe Decisions: [Taking Safe Decisions](#)

RSSB guidance on the management of change (including six complementary Rail Industry Guidance Notes): [Management of Change](#)

4. The role of the assessment body

What is the role of the assessment body?

4.1 The assessment body is appointed by a proposer to carry out independent assessment of:

- how the risk management process in the CSM REA is applied; and
- the results obtained from the risk management process.

4.2 This could involve a sample or vertical audit to check:

- the correct application of the processes to the specific change (but not the question of whether the change is significant or not);
- adequate definition of the part of the system that is being changed;
- robust process for hazard identification and that the hazard identification appears to be complete;
- justified classification of hazards associated with a broadly acceptable risk;
- correctly applied risk acceptance principles (see paragraph 3.25);
- satisfactory demonstration of compliance with safety requirements;
- the hazard record contains the right information about the hazards and their associated safety measures; and the responsibilities of the main parties involved for those hazards; and
- hazards and the associated safety measures are closed and validated.

4.3 To carry out the independent assessment, the assessment body must:

- ensure that it has a thorough understanding of the significant change based on the documentation provided by the proposer;
- conduct an assessment of the processes used for managing safety and quality during the design and implementation of the significant change, if those processes are not already certified by a relevant conformity assessment body; and

- conduct an assessment of the application of those safety and quality processes during the design and implementation of the significant change.
- 4.4 Once the assessment body has completed its assessment as described in paragraph 4.3 it must deliver the safety assessment report as described in paragraph 4.6 below.
- 4.5 The proposer is required to appoint an assessment body at the earliest appropriate stage of the risk assessment process. However, ORR recommends that the assessment body is involved from the beginning of the project so that it can monitor the development of the hazard record, consider other relevant material (such as a safety plan) and possibly ask to observe tests. This may also include the detailed design stage or the manufacturing stage of the project. The assessment body must ensure that its involvement in these activities does not jeopardise its independence. The assessment body's role in oversight does not remove the responsibility of the proposer for overall safety. **In all cases the proposer remains responsible for safety and takes the decision to implement the proposed change.**

Safety assessment report

- 4.6 At the conclusion of the assessment, the assessment body produces a safety assessment report, and this should support the proposer in taking the decision on the safety of the system. If the proposer disagrees with any part of the safety assessment report it must keep a record of this with clear justification for the disagreement.
- 4.7 If the change to the system also requires an authorisation for placing in service, then the safety assessment report should also be submitted to ORR with the technical file and other documentation. ORR will take this into account in considering the authorisation. If there is an authorisation for placing in service and the proposer disagrees with any part of the safety assessment report it must keep a record of this on the technical file with clear justification for the disagreement.
- 4.8 Where an assessment body has delivered a safety assessment report, that report must be mutually recognised by any other assessment body within the UK, providing the system is used under the same conditions and equivalent risk acceptance criteria are applied. The EU will no longer accept safety assessment reports produced by UK AsBos.
- 4.9 In accordance with Annex III of the CSM REA the safety assessment report must contain as a minimum the following information:

- identification of the assessment body;
- the independent assessment plan;
- the definition of the scope of the independent assessment as well as its limitations;
- the results of the independent assessment, including in particular:
 - detailed information on the independent assessment activities for checking the compliance with the provisions of the CSM REA; and
 - any identified cases of non-compliance with the provisions of the CSM REA and the assessment body's recommendations; and
- the conclusions of the independent assessment.

5. Miscellaneous requirements for specific duty holders

Railway undertakings and infrastructure managers

- 5.1 RUs and IMs should undertake periodic audits of the application of the CSM REA as part of their SMS arrangements.
- 5.2 As part of their [annual safety report](#) to ORR, mainline RUs and IMs must include:
- a summary of experience in applying the CSM REA; and
 - a summary report on the decisions related to significance of change.

Entities in charge of maintenance

- 5.3 All ECMs should undertake periodic audits of the application of the CSM REA as part of their maintenance system as referred to in regulation 18A of ROGS.
- 5.4 As part of their annual maintenance report to the certification body, ECMs responsible for freight wagons must include a summary of experience in applying the CSM process.

Supervision by national safety authorities

- 5.5 ORR may check the process that:
- RUs;
 - IMs; and
 - ECMs not responsible for freight wagons but registered in the national vehicle register,

have used to determine how to apply the CSM REA. Proposers must therefore keep a record of how they have arrived at their decisions, particularly in relation to the test for significance.

- 5.6 The process that freight wagon ECMs use may be checked by ORR, or another certification body, as part of its surveillance activities.

Annex A: Determining the significance of a change

A.1 When a proposed change has an impact on safety, the CSM REA requires the proposer to decide, by expert judgement, the significance of the change based on stated criteria (Article 4(2)).

A.2 These criteria are:

- **failure consequence:** credible worst-case scenario in the event of failure of the system under assessment, taking into account the existence of safety barriers outside the system;
- **novelty** used in implementing the change: this concerns both what is innovative in the railway sector, and what is new just for the organisation implementing the change;
- **complexity of the change;**
- **monitoring:** the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;
- **reversibility:** the inability to revert to the system before the change;
- **additionality:** assessment of the significance of the change taking into account all recent safety-related modifications to the system under assessment and which were not judged as significant.

A.3 The CSM REA does not prescribe how to use the criteria, or the priority or weighting given to any of them. The method described here may be useful to proposers and provide some structure for taking these decisions.

Methodology for using the criteria

A.4 It is likely that the proposer will need to undertake some preliminary work to identify and understand the relevant hazards before applying the significance test. A good overall understanding of all the hazards will help with identifying the most appropriate risk acceptance principle.

A.5 For a significant change the proposer must produce “a written declaration that all identified hazards and associated risks are controlled to an acceptable level”. The

proposer must also be confident that risk is controlled to an acceptable level if a change is not significant.

A.6 Taking the criteria together, it would be reasonable to conclude that a change is not significant if the proposer:

- is confident that it has identified all significant hazards (i.e. those that give rise to non-negligible risk); and either
- knows how it will control the associated risk to an acceptable level; or
- is confident that it will be straightforward to identify and implement the measures required to control the associated risk to an acceptable level.

A.7 If the proposer chooses to apply the criteria more explicitly, it is possible to group and sequence the criteria in a way that assists their application.

Additionality

A.8 Additionality is considered first, as this defines the **scope** of the change that is to be assessed.

A.9 When a change 'A' is proposed, other recent changes (B, C, ...) should be considered and, if necessary, included within the scope of the change subject to the test of significance (that is, if necessary, the change whose significance is to be decided is A + B + C ...)

A.10 Additionality can be described as considering other changes that have been made since the entry into force of the CSM REA (23 May 2013) or since the last application of the risk management process (whichever is later).

A.11 This would achieve the intention of the CSM REA (which refers to '**recent**' safety-related changes), whilst being practical and not imposing an arbitrary time limit.

Novelty and complexity

A.12 Novelty and complexity can be thought of as measures of the **uncertainty of outcome** or the likelihood that the proposed change, once implemented, will or will not behave as predicted. Clearly, the more novel and the more complex a change is, the higher the likelihood that it may behave in an unpredicted, and possibly undesirable, way. Therefore, the more novel and the more complex a change is, the more significant it is likely to be.

Failure consequence

- A.13 Failure consequence (or **consequence of failure**) is straightforward. This is asking the question “What is the worst that could happen if the system behaves in an undesirable way following the introduction of the proposed change?”

Combining uncertainty of outcome and consequence of failure

- A.14 Risk is usually understood to be *likelihood x consequence*. Similarly, ‘*uncertainty of outcome*’ x ‘*consequence of failure*’ can be thought of as a factor measuring the potential scale of a change with respect to safety. The ‘uncertainty of outcome’ is judged by reference to novelty and complexity.

Monitoring and reversibility

- A.15 Monitoring and reversibility are additional criteria that should be considered where the decision about whether the change is ‘significant’ or ‘non-significant’ cannot be made on the basis of the ‘*uncertainty of outcome x consequence of failure*’ test.
- A.16 The criterion in relation to monitoring is ‘the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions’. In essence, this is asking the question “Can I see what is going on and react in time?”
- A.17 But a more complex question to ask when thinking about monitoring as a criterion is “Is it possible and practicable to introduce a system of monitoring that gives sufficient warning early enough to permit effective intervention to prevent or mitigate any hazard arising from the change I have made?” Note that it is not sufficient, for example, to simply install monitoring equipment. Supporting operational procedures are necessary to take note of, and react to, warnings generated by the equipment.
- A.18 Reverting to the system before the change is one possible intervention, though one that is not usually available in the case of engineering change. It should therefore be thought of in the wider sense of:

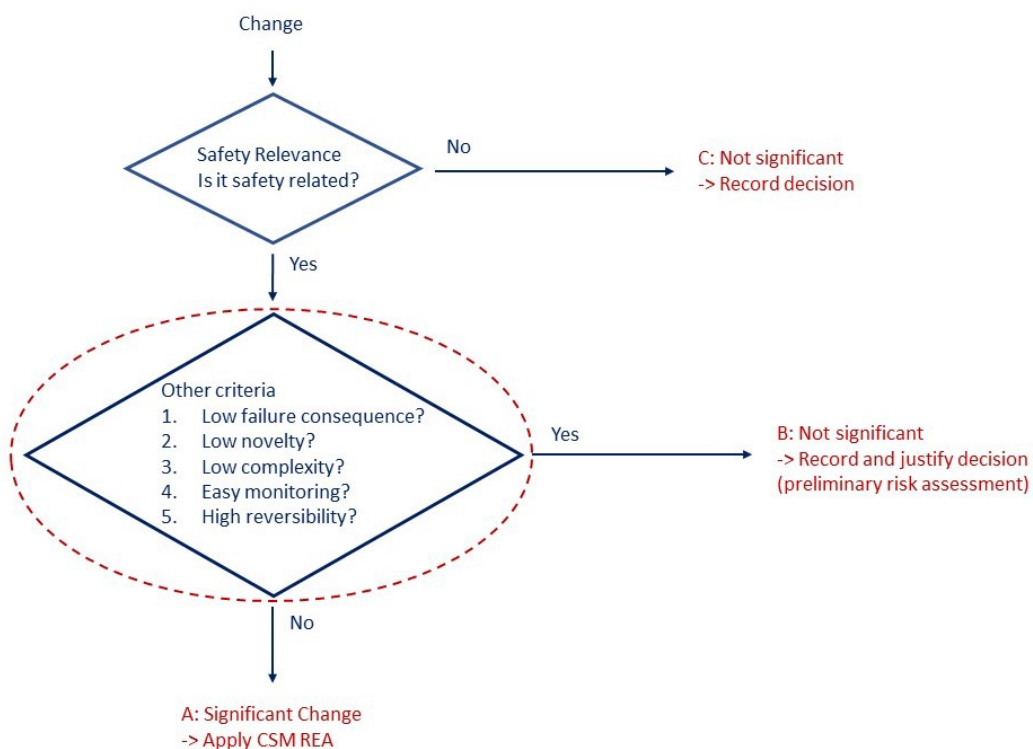
The ability (or otherwise) to intervene in a timely manner to prevent or mitigate any hazard arising from the change you have made, when such intervention is indicated by the monitoring arrangements.

- A.19 If it is not possible to adequately monitor the effects of a change so as to be able to ‘take appropriate interventions’; or if it is impossible to reverse the effects of a change, it is likely that the change should be considered significant.

Judging significance

A.20 By considering these factors cumulatively, a decision can be reached on significance of change. In many cases, just one criteria might be so obviously relevant that it is not necessary to evaluate others. It is possible to develop a simple matrix, to assist in making a judgement about whether a proposed change is 'significant' (high uncertainty, high consequence) or 'non-significant' (low uncertainty, low consequence) or where the additional criteria (ability to monitor and reversibility) need to be applied to make a final decision.

Figure 3: Criteria for assessing the significance of change



Annex B: Criteria for assessment bodies

- B.1 Under the CSM REA, the assessment body must be either:
- (a) accredited by a national accreditation body; or
 - (b) recognised by a recognition body (see below); or
 - (c) the national safety authority (ORR in the UK).
- B.2 In the UK the national accreditation body (the [United Kingdom Accreditation Service](#)) has been asked to establish an accreditation scheme.
- B.3 An assessment body may be accredited or recognised for one, several or all of the following areas of competence:

Accreditation and recognition

- B.4 The assessment body must be accredited or recognised for the different areas of competence within the railway system, or parts of it, for which an essential safety requirement exists. This includes the area of competence involving the operation and maintenance of the railway system.
- B.5 The assessment body must be accredited or recognised for assessing the overall consistency of the risk management and the safe integration of the system under assessment into the railway system as a whole. This must include competence of the assessment body in checking the following:

Organisation

- B.6 The arrangements necessary to ensure a coordinated approach to achieving system safety through a uniform understanding and application of risk control measures for sub- systems.

Methodology

- B.7 Evaluation of the methods and resources deployed by various stakeholders to support safety at sub-system and system level.

Technical aspects

- B.8 The technical aspects necessary for assessing the relevance and completeness of risk assessments and the level of safety for the system as a whole.

B.9 The CSM REA allows the following types of recognition of an assessment body by the National Safety Authority (ORR in the UK):

- (a) an entity in charge of maintenance (ECM);
- (b) an organisation or part of it; or
- (c) an individual;

to conduct independent assessment through the assessment and supervision of the SMS of an RU or an IM;

- recognition by the National Safety Authority (ORR in the UK) as ECM certification body of the ability of:
 - an organisation or part of it; or
 - an individual

to conduct independent assessment through assessment and surveillance of the system of maintenance of an ECM; or

- recognition by a recognition body designated by the UK of the ability of:
 - an ECM;
 - an organisation or part of it; or
 - an individual

to conduct independent assessment.

B.10 In any of the cases above the person acting as assessment body must be sufficiently independent from the project that it is engaged in (see paragraphs 3.64 to 3.74).

B.11 ORR or an ECM certification body must accept accreditation, or recognition, as proof of the ability of:

- an RU to act as an assessment body when granting a safety certificate;
- an IM to act as an assessment body when granting a safety authorisation; or
- an ECM to act as an assessment body when granting an ECM certificate.

Annex C: Guidance on organisational change

Purpose

- C.1 This Annex provides high-level guidance on the application of the CSM REA when assessing significant organisational changes.

What is a significant organisational change?

- C.2 It is a requirement of the CSM REA that, when making any technical system, operational or organisational changes which could impact on the safety of the operational railway system, consideration should be given to whether or not the change is 'significant' by applying the six criteria described in the CSM REA.
- C.3 The reasons for the decision that a change is, or is not, significant must be documented. The documentation of this assessment is particularly important where it is decided that a change is not significant, as this may be required to be reviewed should the change be implicated in a safety incident in the future.
- C.4 It is not possible to define explicitly what a significant organisational change is in terms of a particular type of change. A change that is significant for one company/circumstance may not be significant for another company/circumstance. Each change must be assessed individually in the context in which it is being applied.
- C.5 The first consideration is whether the organisational change is within the scope of the CSM REA – could it impact on the operational or maintenance processes of the railway system?
- C.6 The second consideration is whether the change affects safety, either directly or indirectly. If the organisational change does not affect safety, then no further consideration needs to be given in relation to the application of the CSM.
- C.7 If an organisational change does affect safety, one method for assessing whether a change is significant is offered in Annex A of this guidance.

Assessing the change

- C.8 The CSM REA presents three 'risk acceptance principles' by which the hazards associated with a significant change can be analysed and evaluated. These are:

- the application of codes of practice;
- a comparison with similar systems (reference systems); and
- an explicit risk estimation.

C.9 The most likely acceptance principle to be applied to significant organisational change is explicit risk estimation. This can be qualitative. Quantitative risk assessment of the proposed organisational change is not necessarily required.

C.10 Risk assessment associated with significant organisational changes is not an exact science; it is about managing and organising people, therefore a qualitative or semi-quantitative risk ranking method for assessing organisational changes should meet the requirements of the CSM REA.

C.11 Most companies already have structured safety validation processes for organisational changes within their existing SMSs which are likely to meet the requirements of the CSM REA. In broad terms, for significant organisational changes this would include:

- definition of the extent of the change being made;
- preparation of disposition statements indicating where the safety responsibilities are transferred from one job description to the job description of the new role;
- checking that the new job roles specify the correct competency levels for the safety functions that have been transferred;
- carrying out a risk assessment commensurate with the scale of the change to determine the potential impact of the change and that adequate mitigation measures have been put in place;
- recording and maintaining the outputs of the risk assessment in a hazard record;
- establishing the go-live criteria that need to be achieved before the organisational change is implemented; and
- documentation of records relating to the bullet points above.

Risk Acceptance criteria

- C.12 The quantitative risk acceptance criteria defined in paragraph 2.5.4 of Annex I of the CSM REA only apply to significant changes relating to technical systems and therefore do not have to be considered in the context of significant organisational changes.

Mutual recognition

- C.13 One of the main principles introduced by the CSM REA is that of mutual recognition. This principle is designed to reduce industry costs by not having to redo risk assessment work when the change can be applied to more than one company in the UK. Following EU Exit, EU Member States will no longer accept safety assessment reports produced by UK AsBos. Once a significant change has been assessed and subject to an independent assessment by an assessment body in the UK, the change should be acceptable by another assessment body within the UK without additional assessment, providing the same application conditions apply.

Independent Assessment

- C.14 The CSM REA requires that all significant changes, including organisational changes, are independently assessed by an assessment body, which produces a safety assessment report.
- C.15 The role and requirements of an assessment body are described in Chapter 4 of this guidance. The key to a successful independent assessment is getting the assessment body involved at the early stages of the risk assessment process, including attendance at some or all of the workshops/safety review meetings, as long as independence is maintained, and they don't become involved in the design of the change. This will ensure that the assessment body has a good insight into the risk assessment process and the development of the hazard records. Early feedback from the assessment body can help in the development and refining of the risk assessment process being used.
- C.16 The assessment body is required to review the adequacy of the risk assessment process used and determine if the conclusions of the assessment are reasonable based on the results obtained from the assessment. The assessment body does not sign off that the change being made is acceptable from a safety risk perspective. This remains the responsibility of the proposer of the change.

Documentation

C.17 All stages of the application of the CSM REA should be documented and the hazard record established for use through the implementation of the change.

Risk assessment process

C.18 There is no defined methodology currently available for risk assessment of organisational change. A qualitative risk assessment based on a structured workshop process and the management of a hazard record derived from the workshops should be adequate to meet the requirements of the CSM REA.

Annex D: Glossary of terms and acronyms

Accreditation

An attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity

Accreditation

An attestation by a national accreditation body that a conformity assessment body meets the requirements set by harmonised standards and, where applicable, any additional requirements including those set out in relevant sectoral schemes, to carry out a specific conformity assessment activity

Advanced stage of development

When the proposer considers that the planning/construction stage of a project has reached a point where a change in the technical specifications would not be viable on economic, contractual, legal, social or environmental grounds

ApBo

Approved Body

Approved Body

A body that has been approved by the Secretary of State to carry out the GB verification assessment procedure to ensure compliance with the relevant NTSNs. ApBos provide

independent certification of specific stages in the project lifecycle on conformity to required NTSNs. They produce a Certification of Verification (CoV) re the national rules against which conformity has been examined, and can optionally also produce Intermediate Statements of Verification (ISVs)

AsBo

Assessment Body

Assessment Body

The independent and competent external or internal individual, organisation or entity which undertakes investigation to provide a judgement, based on evidence, of the suitability of a system to fulfil its safety requirements.

Code of Practice

A written set of rules that, when correctly applied, can be used to control one or more specific hazards.

DeBo

Designated Body

Designated Body

A person appointed under regulation 31 of RIR as a designated body

ECM

Entity in Charge of Maintenance

Entity in Charge of Maintenance

Any person or organisation that is responsible for the safe maintenance of a vehicle and is registered as an ECM in the national vehicle register. This can include people or organisations such as transport undertakings, infrastructure managers, a keeper (usually the

	owner of a rail vehicle) or a maintenance organisation
ETCS	European Train Control System
Functional sub-systems	Traffic operation and management; maintenance; and telematics applications for passenger and freight services
Hazard	A condition that could lead to an accident
Hazard identification	The process of finding, listing and characterising hazards
Hazard record	The document in which identified hazards, their related measures, their origin and the reference to the organisation which has to manage them are recorded and referenced
IM	Infrastructure Manager
Interfaces	All points of interaction during a system or sub-system life cycle, including operation and maintenance where different actors of the rail sector will work together in order to manage the risks
Interoperability constituent	Any elementary component, group of components, subassembly or complete assembly of equipment that is incorporated or intended to be incorporated into a sub- system upon which the interoperability of the rail system depends directly or indirectly; and the concept of a “constituent” covers both tangible objects and intangible objects such as software

National Accreditation Body

The sole body in the UK that performs accreditation in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9th July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93

National vehicle register

A database of vehicles authorised or operated in Great Britain under RIR

NTRs

National Technical Rules

National Technical Rules

National Technical Rules setting out standards, technical specifications and technical rules in relation to the rail system, as amended or varied from time to time, a list of which is published by the Secretary of State in accordance with regulation 3C of the Railways Interoperability Regulations 2011

NTSN

National Technical Specification Notice

National Technical Specification Notice

A notice published by the Secretary of State pursuant to regulation 3B of the Railways Interoperability Regulations 2011 setting out the standards, technical specifications and technical rules in use in the United Kingdom as amended or varied from time to time

NSA

National Safety Authority

Proposer

One of the following:

(a) a railway undertaking or an infrastructure manager;

(b) an entity in charge of maintenance;

(c) a contracting entity or a manufacturer which invites an approved body or a designated body to apply the UK verification assessment procedure in accordance with Regulation 17 of and Schedule 4 to the Railways (Interoperability) Regulations 2011;

(d) an applicant for an authorisation for the placing in service of structural sub-systems

RAC

Risk Acceptance Criteria

Risk Acceptance Criteria

The terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further.

Recognition

An attestation by a national body other than the national accreditation body that the assessment body meets the requirements set out in Annex II to the CSM REA to carry out the independent assessment activity specified in Article 6(1) and (2)

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

RGS	Railway Group Standard
RIR	The Railways (Interoperability) Regulations 2011
Risk	The frequency of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm
Risk acceptance criteria	The terms of reference by which the acceptability of a specific risk is assessed; these criteria are used to determine that the level of a risk is sufficiently low that it is not necessary to take any immediate action to reduce it further
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 estimation	The process used to produce a measure of the level of risks being analysed, consisting of the following steps: estimation of frequency, consequence analysis and their integration

Risk evaluation	A procedure based on the risk analysis to determine whether an acceptable level of risk has been achieved
Risk management	The systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling risks
ROGS	The Railways and Other Guided Transport Systems (Safety) Regulations 2006
RSSB	Rail Safety and Standards Board
RU	Railway Undertaking (also referred to as Transport Undertaking under ROGS)
Safe integration	The action to ensure that incorporating an element of a system into a bigger system does not create an unacceptable risk for the resulting system
Safety	Freedom from unacceptable risk of harm
Safety assessment report	The document containing the conclusions of the assessment performed by an assessment body on the system under assessment
Safety Management System	The organisation and arrangements established by an infrastructure manager or a railway undertaking to ensure the safe management of its operations

Safety Measures	A set of actions either reducing the frequency of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk
Safety Requirements	The safety characteristics (qualitative, quantitative, or both) necessary for the design, operation (including operational rules) and maintenance of a system in order to meet legal or company safety targets
SFAIRP	So far as is reasonably practicable
SMS	Safety Management System
Structural sub-systems	Rolling stock; infrastructure; control, command and signalling; and energy
Sub-system	The whole, or, as the context requires, part of a subdivision of the rail system as specified in sections 1(a) and 1(b) of Schedule 3, namely structural subsystems and functional subsystems and includes a structural or functional subsystem that is intended to become the whole or part of a subdivision of the rail system
System	Any part of the railway system which is subjected to a change whereby the change may be of a technical, operational or organisational nature
Systematic failure	A failure that occurs repeatedly under some particular combination of inputs or under some particular environmental or application conditions

Systematic fault

An inherent fault in the specification, design, manufacturing, installation, operation or maintenance of the system under assessment

Technical system

A product or an assembly of products including the design, implementation and support documentation; the development of a technical system starts with its requirements specification and ends with its acceptance; although the design of relevant interfaces with human behaviour is considered, human operators and their actions are not included in a technical system; the maintenance process is described in the maintenance manuals but is not itself part of the technical system

TVM

Transmission Voie-Machine (*English: track-to-train transmission*). A form of in-cab signalling used on high speed railway lines originally deployed in France

Annex E: Table of updates to guidance

Paragraph number	Change	Updated text
Background	Revised wording	Amended wording to clarify significance of CSM-REA when any technical, operational or organisational change is being proposed on the mainline railway.
Paragraph 1.4	New paragraph	New text explaining changes made to the CSM REA following EU Exit.
Paragraph 2.4	New paragraph	New text confirming requirement to ensure all health and safety legal requirements are met.
Paragraph 2.6	New paragraph	New text confirming that non-mainline operators must meet the requirements in Schedule 4 of ROGS.
Paragraph 2.18	New paragraph	New text explaining that NTSNs have replaced TSIs from 1 January 2021.
Figure 1	Updated text	The text in the boxes has been updated to improve clarity.
Paragraph 3.26	Deleted text	The reference to mutual recognition between the UK and EU Member States has been removed, following EU Exit.
Paragraph 3.33	New text	Additional text to make clear that fire safety is important, and that operators need to ensure they identify fire safety standards for their work.
Paragraph 3.49	Deleted text	Removal of previous wording that allowed risk acceptance criteria to be based on EU legislation.

Paragraph number	Change	Updated text
		Removal of further text to improve clarity.
Paragraph 3.49	Moved paragraph / new text	Previous paragraph 3.49 moved to paragraph 3.51. New paragraph 3.49 added to bring clarity on harmonised design targets.
Paragraph 3.50	Moved paragraph / new text	Previous paragraph 3.50 moved to paragraph 3.52. New paragraph 3.50 added to provide further information on the use of harmonised design targets.
Paragraph 3.51	Deleted text / new paragraph	Original text on critical accident deleted / moved to paragraph 3.52. Paragraph 3.51 now contains text on catastrophic accident.
Paragraph 3.52	Deleted text	Deletes reference to use of harmonised design targets when mutual recognition in an EU Member State is proposed. Mutual recognition between the UK and an EU Member State is no longer possible after EU Exit.
Paragraph 3.52	Moved paragraph	Paragraph 3.52 now covers critical accident. Text from previous paragraph 3.52 now incorporated in paragraph 3.50 on harmonised design targets.
Paragraph 3.69	New text	Replacement text to clarify what assessment bodies should consider when looking at a significant change, and explaining that the option to apply relaxed criteria is no longer possible.

Paragraph number	Change	Updated text
Paragraph 4.8	New text	New wording to confirm that the EU will no longer accept safety assessment reports produced by UK AsBos.
Paragraph 5.4	Deleted text	Text deleted as ECMs are no longer required to share information with the EU.
Paragraph 5.5	Deleted text	Text deleted as EU National Safety Authorities are no longer able to supervise process used to apply the CSM REA to Railway Undertakings, Infrastructure Managers and Entities in Charge of Maintenance in the UK.
Figure 3	Deleted	Figure 3 in the previous version of this guidance document has been deleted. It set out a proposed approach to applying criteria for determining the significance of a change, but was confusing because it was only one possible approach. The subsequent figures have been renumbered.
Figure 4	Amended text	
Annex B – text below paragraph B3	Deleted text	Removal of text on use of relaxed criteria as this is no longer possible after EU Exit.
Annex 3 – relaxed criteria where a significant change is not mutually recognised	Deleted text	Annex 3 in the September 2018 version of this guidance document has been deleted. Mutual recognition between the UK and EU Member States is no longer possible after EU Exit. The subsequent annexes have been renumbered.

Paragraph number	Change	Updated text
Annex C – guidance on organisational change – paragraph C18	New text	Text added to confirm that EU Member States will no longer accept safety assessment reports produced by UK AsBos after EU Exit.
Annex 5	Deleted text	Annex 5 in the September 2018 version of this guidance document has been deleted. The example given is now out of date.



© Crown copyright 2024

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at orr.gov.uk

Any enquiries regarding this publication should be sent to us at orr.gov.uk/contact-us

