ORR guidance on the application of the common safety method (CSM) on risk evaluation and assessment

December 2012
Second edition published by the Office of Rail Regulation, December 2012

This guidance is issued by the Office of Rail Regulation. Following the guidance is not compulsory and you are free to take other action. But if you do follow the guidance you will normally be doing enough to comply with the law. Railway inspectors seek to secure compliance with the law and may refer to this guidance as illustrating good practice.
## Contents

1. Introduction 4

2. Applying the Common Safety Method (CSM) 6
   - Who has duties under the CSM? 6
   - What parts of the rail system are exempt? 6
   - What type of changes does the CSM apply to? 7
   - Determining the significance of a change 8

3. The risk assessment process. 10
   - Preliminary system definition 10
   - System definition 10
   - Hazard Identification 11
   - Codes of Practice 13
   - Reference systems 14
   - Explicit risk estimation 15
   - Hazard record 16
   - Other documentation 17
   - Demonstration of system compliance 17
   - Independent assessment 18
   - Avoiding duplication of assessment processes 18
   - What is the role of the Assessment Body? 19

4. Miscellaneous requirements of the Regulations 21
   - Annex 1 Determining the significance of a change 22
   - Annex 2 – Risk management process and independent assessment 27
   - Annex 3 – Criteria which must be fulfilled by assessment bodies 28
   - Annex 4 Guidance on organisational change 29
1. Introduction

1.1 This guidance summarises the European Commission Regulation that sets out a common safety method (CSM) on risk evaluation and assessment for the mainline railway industry. It explains the main requirements of the Regulation, to whom it applies, and specific points on compliance in the UK.

This is the second issue of the guidance. It has been updated to reflect the coming into force date for the CSM to apply to all significant safety-related changes, some revisions to the original CSM and developments in other legislation. It will continue to be updated as further revisions to the CSM come into force or if there are changes to other processes that impact on how the CSM should be applied. For example, proposals to amend the Regulation were made by ERA to the Commission in July 2012. These include a system of authorisation for assessment bodies for cross-border projects. This guidance will be updated when the new provisions have been agreed.

1.2 The full text of the Regulation is available on the EC Website (http://eur-lex.europa.eu/JOHtml.do?uri=OJ%3AL%3A2009%3A108%3ASOM%3AEN%3AHTML). As a European Commission (EC) Regulation, it applies directly and does not need to be transposed into UK law. The Regulation primarily applies to railway undertakings (RUs) and infrastructure managers (IMs) but also applies to project entities and manufacturers in certain circumstances (see paragraphs 2.5 - 2.6).

1.3 The European Rail Agency (ERA) has also produced guidance for the Regulation. This is in two parts; the first part is intended as further explanation to the Regulation – ‘Guide to the Application of the CSM’ (http://www.era.europa.eu/Document-Register/Documents/guide-for-application-of-CSM-Ver-1-1.pdf); the second ERA guidance document is a collection of examples of risk assessments / processes / applications that have been used in some Member States prior to the introduction of the CSM (http://www.era.europa.eu/Document-Register/Documents/collection_of_RA_Ex_and_some_tools_for_CSM_V1.1.pdf). The main aim of the second part is to illustrate the types of tools and techniques that may be used with the CSM.

1.4 The Regulation is part of a wide-ranging programme of work by ERA and the EC to bring about a more open, competitive rail market while seeking to ensure that safety levels are maintained, and, if reasonably practicable, improved. In the past, safety requirements may have been used as a barrier to open competition across the EU. The intention of this Regulation is to harmonise processes for risk assessment and evaluation (for significant changes) and the evidence and documentation produced during the application of these processes. By doing this, it should be easier for an assessment undertaken in one Member State to be accepted in another with the minimum of further work. This is referred to as mutual recognition.

1.5 The process set out in the Regulation is intended to complement requirements in other legislation, for example on interoperability or safety certification, and not to duplicate them. The broad principles of how the requirements fit together are provided in the following paragraphs.

1.6 The Railway and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS), as amended, require RUs and IMs to develop their safety management system (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. ORR will check compliance with this when we examine applications from duty-holders for safety certificates or authorisations and when we subsequently supervise those duty-holders.
Currently ORR is consulting on revisions to ROGS which will remove the requirement for a written safety verification scheme by RUs or IMs in certain circumstances. It will not be necessary to carry out separate processes if and when this change to ROGs comes into force.

There are other laws in the UK that require risk assessments to be undertaken, such as the Management of Health and Safety at Work Regulations. The CSM meets the requirements that are within the scope of the CSM, so further analysis may need to be done to cover aspects of risk assessment beyond that specifically required by the CSM. However, there is no need to duplicate aspects of risk assessment covered by the CSM.

Some changes to the railway system will also trigger the requirements of the Railways (Interoperability) Regulations (RIR) 2011. The aim of interoperability legislation is to achieve a technical and operational harmonisation of the main structural and functional railway subsystems. The structural subsystems are:

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

The functional subsystems are:

- traffic operation and management;
- maintenance; and
- telematics applications for passenger and freight services.

The CSM applies to significant changes to all railway sub-systems, significant changes to the operation of the railway, and significant organisational changes that could impact on the operating conditions of the railway system.

The CSM is a framework that describes a common mandatory European risk management process for the rail industry and does not prescribe specific tools or techniques to be used. Risk assessment is a familiar concept in the UK and ORR's experience is that the principles of the Regulation are already being applied for most projects. We therefore do not expect its introduction to require major changes in approach. However, some adjustment of processes for projects may be needed. For example, the requirements for independent assessment may require changes and the use of risk acceptance criteria for technical systems may be new.

The CSM framework 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);
- explicit risk estimation.
2. Applying the Common Safety Method (CSM)

2.1 The CSM Regulation came fully into force on 1 July 2012. The Regulation applies to all significant safety-related technical, operational and organisational changes.

2.2 For those projects at an ‘advanced stage’ on 1 July 2012 the Regulation does not have to be applied. Projects can be considered to be at an advanced stage if amendments to the design would be either not technically feasible or not economically viable.

Who has duties under the CSM?

2.3 The Regulation 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.

2.4 In many circumstances, proposers will be RUs or IMs. This aligns with the Safety Directive 2004/49/EC which places the main responsibilities for safety on these two key players.

2.5 However, the CSM Regulation allows other bodies to act as the proposer. This applies particularly to project entities and manufacturers who lead projects where they are required to engage a Notified Body (NoBo), and rail vehicle projects that require authorisation to place into service under interoperability.

2.6 A manufacturer may want to place a new or altered product or system on the market. This may require the application of the CSM and an authorisation to place into service under interoperability. The manufacturer may therefore choose to act as the proposer. However, the change for which the manufacturer is the proposer is complete once the product is placed on the market. An RU or IM wishing to use the new or altered product or system in a specific application or location will be the proposer of a new change. The RU/IM may use the manufacturer’s authorisation as part of their own application of the CSM and the additional work needed under the Regulation will focus on route-specific technical compatibility and safe integration.

2.7 Other bodies in the rail sector – such as suppliers and service providers – may need to participate in the process. This involvement should be coordinated by the proposer, possibly supported by contractual arrangements.

What parts of the rail system are exempt?

2.8 The CSM Regulation has the same scope of application as the Railway Safety Directive. Therefore, the regulation does not apply to:

- metros, trams, and other light rail systems;
- networks that are functionally separate from the rest of the railway system and intended only for the operation of local, urban or suburban passenger services, as well as railway undertakings operating solely on these networks;
• privately owned railway infrastructure that exists solely for use by the infrastructure owner for its own freight operations;

• heritage vehicles that run on national networks providing that they comply with national safety rules and regulations with a view to ensuring safe circulation of such vehicles;

• heritage, museum and tourist railways that operate on their own network, including workshops, vehicles and staff.

What type of changes does the CSM apply to?

2.9 The CSM applies to significant safety-related technical, operational or organisational changes to the railway system. The test for ‘significance’ is examined at paragraph 2.22 below.

Technical changes

2.10 Technical changes are changes to a structural railway sub-system. Technical changes should also be reviewed to determine whether they introduce changes to the operation of the railway sub-system under consideration.

Operational changes

2.11 Operational changes are:

i. changes to the operation of a structural railway sub-system; or

ii. changes to the operation of the railway system; or

iii. changes to the operating rules of the railway system.

2.12 Changes to the operation of a structural railway sub-system are often caused by technical changes to that sub-system. In this case, the technical change and its effect on the operation of the railway sub-system, and any changes to the operation of the railway system or to the operating rules of the railway system, should be assessed together.

2.13 Technical changes are very rarely introduced ‘for their own sake’. They are introduced for variety of reasons; on most occasions, one of the reasons for introducing technical change will be to increase capacity on a part of the railway system (an operational benefit).

2.14 For example, if a twenty-kilometre stretch of railway line were re-doubled, including changes to the control-command signalling (CCS), this is a significant safety-related technical change that should be assessed in accordance with the CSM. For such a change, there are also likely to be changes to the operation of the CCS sub-system as a result of technical changes to the sub-system; these operational changes would be assessed together with the significant safety-related technical changes as part of the risk assessment required under the CSM.

2.15 If an RU decides to run two or three times more trains per hour on the re-doubled line, this is a change to the operation of that part of the railway system. This operational change is safety-related and may also be significant because it introduces new risk scenarios, such as derailments that block the adjacent line. This operational change should be assessed together with the technical change and the changes to the operation of affected structural railway sub-systems.

2.16 Technical changes to a sub-system can also introduce changes to the operating rules of the railway system. On the GB mainline railway, these would be changes to the Rule Book and other National Operations Publications.
2.17 Changes to the operating rules of the railway system should be considered together with the technical change, the change to the operation of the affected railway sub-system and any change to the operation of the railway system.

2.18 However, changes to the operation of the railway system, or changes to the operating rules of the railway system, can be introduced without a related technical change. The CSM should be used to assess whether these changes, if they are safety-related, are significant or not. If they are significant, the CSM should be applied to these changes.

Organisational changes

2.19 Organisational changes are changes to the organisation of an actor in the railway system which could impact on the safety of the railway system. The ‘actor’ is most likely to be an IM or a RU, but it could be an entity in charge of maintenance (ECM) or any other organisation that affects the safety of the railway system.

2.20 For example, a change to the safety management system such as 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 could be a significant safety-related change and should be assessed using the CSM.

2.21 Guidance on organisational changes can be found at Annex 4.

Determining the significance of a change

2.22 The CSM Regulation applies to ‘significant’ safety-related changes. To determine whether a change is significant or not, the proposer needs to examine the criteria in the Regulation (See Annex 1). Note that the assessment body (see paragraphs 3.67 - 3.70) checks the whole CSM process but cannot question the proposer’s decision to apply the CSM.

2.23 If a change is deemed to be non-significant, then a proposer is not required to apply the CSM and the change should be managed under the change management processes as described in the proposer’s SMS. Risk assessment may also be required as part of compliance with other Regulations such as Management of Health and Safety at Work Regulations 1999, but the assessment does not have to follow the CSM process.

2.24 ORR, or the safety authority in another EU member state, may check the process that RUs or IMs have used to determine whether or not to apply the CSM. It is very important, therefore, for proposers to document their decisions, particularly in relation to the test for significance.

2.25 The Regulation 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.

2.26 The regulation gives no order or priority on how to use the “significance” criteria, nor any thresholds to evaluate and make the decision. To help proposers work through the process, a UK industry proposal for how to determine significance is included at Annex 1. This approach is one way of applying the criteria and is not mandatory.

Additionality
2.27 Additionality can be described as considering other changes that have been made ‘recently’, 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.

2.28 One difficulty in examining a series of non-significant safety-related changes is determining what is meant by ‘recent’. Annex 1 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.

2.29 Breaking down a significant change into a series of smaller changes, which individually are not significant so that the CSM is then not applied to the overall significant change, is not permitted by the Regulation.

Novelty and complexity
2.30 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 lead to an increase in safety risk. Classifying such changes as significant and applying the CSM, 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. The risk assessment process.

The main phases of the CSM process are illustrated in the diagram in Annex 2. The process illustrated is not static or linear as the proposer may undertake iterations of all or part of the process. It ends when the proposer is content that for each hazard, compliance has been achieved with the identified safety requirements and measures by the application of defined risk acceptance principles. See paragraphs 3.23 to 3.52 below.

The processes required by the Regulation 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 Regulation should review their current processes and procedures and make any necessary adjustments.

Preliminary system definition

3.1 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
- address the information described in paragraph 3.4 (a) to (d) to the extent necessary to enable the proposer to determine the significance of the change.

System definition

3.2 The CSM 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.

3.3 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.

3.4 The Regulation 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;

(g) assumptions which shall determine the limits for the risk assessment.

3.5 The system definition needs to cover not only normal mode operations but also degraded or emergency mode.

3.6 Consideration of interfaces should not be restricted to physical parameters, such as interfaces between wheel and rail. It should include human interfaces, for example 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.

3.7 Operational procedures and rules, and staff competence should be considered as part of the system environment in addition to the more usual issues such as weather, electromagnetic interference, local conditions such as lighting levels etc.

3.8 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.

3.9 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). 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.

3.10 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**

3.11 The purpose of the Hazard Identification is to identify all reasonably foreseeable hazards which are then analysed further in the next steps.

3.12 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
• relevant and foreseeable system failure modes.

3.13 While the Regulation does not require that any specific tools should be applied, many of the more well known techniques will be relevant, including: structured brainstorming; checklists; task analysis; hazard and operability studies (HAZOPs); hazard identification studies (HAZIDs); and failure mode and effects analysis (FMEA).

3.14 Whichever technique is used, it is important to have the right mixture of experience and competence while maintaining impartiality and objectivity. A correct hazard identification will underpin the whole risk assessment process and give assurance that the risks will be managed in the project.

3.15 The Regulation uses the term ‘broadly acceptable’1 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 (eg. earthquakes if in a low vulnerability area) or where there is a credible failure mode but the consequences are negligible. 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.

3.16 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 it can be successfully demonstrated that a hazard can be controlled by application of one of the three risk assessment principles required by the Regulation (see paragraph 3.21), following a high level hazard identification, then no further hazard identification is necessary. If it is not possible to have sufficient confidence at this stage, then further analysis of the causes of these high level hazards is undertaken to identify relevant measures to control the risks arising. The risk assessment process continues until it can be shown that the overall system risk is controlled by one or more of the risk assessment principles.

3.17 Hazard identification is still necessary for those changes where the hazards are 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. This will also support mutual recognition and transparency. 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.

1 ‘Broadly acceptable’ in the Regulation does not have the same meaning as it has in the HSE tolerability of risk framework (see ‘Reducing Risks, Protecting People’)

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.

3.18 Hazards can be analysed and evaluated using one or more of the following principles:

• the application of codes of practice;

• a comparison with similar systems (reference systems); or

• an explicit risk estimation.

3.19 These are termed ‘risk acceptance principles’ in the CSM Regulation.
3.20 In the UK, you can choose any of these three risk acceptance principles. However, if a proposer is seeking mutual recognition in another Member State (MS), they should check whether there is a notified national rule in that MS restricting the choice of risk acceptance principle. If there is, that risk assessment principle will need to be used.

3.21 Individual hazards can be closed out by the application of one of the three principles but it is likely that, for most major projects, a combination of the three principles will be used. Any risk assessment conducted under the CSM should always be proportionate to the extent of the risk being assessed.

3.22 The CSM 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 means that the risk has been reduced to an acceptable level. In these circumstances, ORR will not normally require further evidence that the residual risk is acceptable.

**Codes of Practice**

3.23 Standards and rules have to meet all the following criteria to be used as a code of practice for the CSM Regulation:

- 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 publicly available.

Note: Documents that are publicly available are not necessarily free of charge.

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

- TSIs or other mandatory European standards, for example those used in other EC verifications;
- notified national safety rules (including national legislation that has been notified);
- notified national technical rules.

3.25 Domestic or UK standards can also be used where they meet the requirements in paragraph 3.26. In particular, Railway Group Standards (RGSs) are publicly available and widely acknowledged in the UK railway industry. There are a number of other domestic standards that are publicly available to all railway actors that could be considered as codes of practice in certain circumstances. For example:

- ATOC standards for passenger rail services or passenger rail vehicles;
- Network Rail Company Standards, which are publicly available via IHS UK;
- The Mechanical and Electrical Engineers Networking Group produces codes of practice for the rail industry relating to plant;
- Railway-specific British Standards issued by the British Standards Institution.

This list is not exhaustive.

3.26 It is also possible to use standards or codes of practice from other sectors eg aviation, maritime, etc. but these have to be justified and be acceptable to the assessment body (see paragraphs 3.58 -
3.70). The proposer will have to demonstrate that they are effective in controlling the risks from the relevant hazards in a railway context.

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

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

3.28 In evaluating whether a code of practice controls one or more of the hazards, proposers will need to check that it covers the intended technical application of the system under assessment.

3.29 A document is ‘publicly available’ if it is available without restrictions on who may access it or buy it. This does not necessarily mean free of charge.

3.30 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 TSIs and Railway Group Standards include a process for deviating from them. For example, a Railway Group Standard deviation certificate could be used as part of the demonstration that the system maintains the same level of safety.

3.31. 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, the proposer may have to conduct an explicit risk estimation on those hazards where the code of practice is not relevant for the control of the hazards in the system under assessment. Alternatively, other codes of practice or reference systems could be used.

Reference systems

3.32 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:

- It has been proven in use and has an acceptable safety level;
- it is accepted in the Member State where the change is to be introduced; and
- the system being assessed is used under similar functional, operational and environmental conditions and has similar interfaces as the reference system.

3.33 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 application of it.

3.34 If the reference system meets the requirements in paragraph 3.32, and those in paragraph 3.33 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

3.35 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).

3.36 The estimation can be qualitative, semi-quantitative or quantitative. The choice will be determined by factors such as availability of, and confidence in, quantitative data and the depth of analyses should be proportionate to the potential risks. Any risk assessment should follow a systematic and structured process.

3.37 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 and 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
- 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. Particularly where the assessment is quantitative and where different safety measures need to be evaluated, the results may also need to be accompanied by sensitivity and uncertainty analyses.

3.38 Explicit risk estimation can be used where:

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

3.39 The CSM does not impose any specific tools and techniques to be used in an explicit risk estimation. Proposers may find those outlined in three key documents produced by the UK rail industry or standards committees useful:

- Guidance on preparing and using company risk assessment profiles for transport operators. RSSB Issue1 2009 www.safetyriskmodel.co.uk
• EN50126:1999 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS) applicable to electro and electro-mechanical subsystems.

3.40 For rail vehicles and structural sub-systems, document 1 in paragraph 3.39 provides guidance on the use of the Safety Risk Model (SRM) templates as the framework for the risk assessment.

3.41 Risk Acceptance Criteria for explicit risk estimation. Risk acceptance criteria (RAC) are used to judge whether the risk is sufficiently reduced to allow the proposer to accept and implement the change. RAC can be based on domestic or European legislation. For the UK, this will mean that risks should be reduced ‘so far as is reasonably practicable’ (see ORR SFAIRP guidance on the website at: http://www.rail-reg.gov.uk/upload/pdf/rgd-2009-05.pdf)

3.42 An important exception relates to the RAC for technical systems (RAC-TS) in the Regulation. Proposers should first consider:

• whether the change relates to a technical system for which a functional failure has a direct potential for a catastrophic consequence; and, if so
• if the change needs to be mutually recognised by other member states or the proposer wishes to use the RAC as the acceptance criteria.

3.43 If both apply, then where the proposer demonstrates that the railway sub-system being assessed has a failure rate no greater than $10^{-9}$ per operating hour, then that sub-system must be mutually recognised in other member states, providing the operating conditions and interfaces in those countries are the same as those assumed in the analysis of the sub-system (with the exception at paragraph 3.45).

3.44 Demonstrating compliance with the RAC-TS means that the proposer does not have to undertake further assessments to show that risk has been reduced so far as is reasonably practicable.

3.45 The Regulation allows the application of a less demanding risk acceptance criterion for these functions if the proposer can show that the national safety level in the Member State can be maintained. This can be done by showing that the railway sub-system complies with domestic risk acceptance criteria. In the UK, this means the proposer will need to demonstrate that the risk is reduced so far as is reasonably practicable. In these circumstances, if the railway sub-system is subsequently put on the market or operated in another member state, further demonstrations may be required.

3.46 It is possible for a member state to notify a national rule to ERA which would require a more demanding criterion than $10^{-9}$/operating hour. The UK has no such national rule and at 1 December 2012, our understanding is that no other member state had notified a rule.

Hazard record

3.47 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 Regulation requires that it contains certain information but does not mandate any particular format.
3.48 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 actors in charge of controlling each hazard.

3.49 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 NSA as part of its inspection of a duty holder’s SMS.

3.50 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.

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

3.52 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**

3.53 The Regulation places some minimum requirements on proposers to document certain information to assist the assessment body (see paragraphs 3.58 - 3.70):

- a description of the organisation and the experts appointed to carry out the risk assessment process;
- and
- 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.

**Demonstration of system compliance**

3.54 The proposer ‘accepts’ the change in the system and is responsible for its safe integration and operation. 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 which they are responsible.

3.55 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 and if that happens it should be recorded as such in the hazard record. Contracts may be required to reflect these agreements.
3.56 Many hazards, and the risks arising, will be at shared interfaces and co-operation will be needed to ensure that such risks are properly assessed and controlled.

3.57 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 subsystems so that they can take the appropriate action.

Independent assessment

3.58 The Regulation requires an independent assessment of how the risk management process is applied and of the results. The proposer is able to choose (subject to certain restrictions) the assessment body (AB), unless there is a national rule in a Member State that requires certain bodies or persons are used. There is no such national rule in the UK.

3.59 The AB must meet the criteria set out in the Regulation (included in this guidance at Annex 3). The proposer can appoint an external body or an in-house service. Factors that enable the proposer to demonstrate that an in-house AB is independent include:

- Different line management;
- No involvement with the development of the safety measures associated with the system under assessment;
- Freedom from commercial influence or bias.

3.60 The scale and complexity of any given project may determine whether an external or in-house AB 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.

3.61 The process for taking the decision about use of internal or external assessment should be recorded. Relevant factors include:

- evidence to satisfy the proposer that the AB is independent and competent;
- absence of financial pressure or incentives on the AB (noting that the proposer cannot control financial pressure or incentives from third parties);
- checks that the AB has civil liability insurance, if it is an external organisation; and
- appropriate policies relating to confidentiality rules, if the AB is an external organisation.

3.62 Revisions to the CSM relating to the role, competence and accreditation of Assessment Bodies were proposed by ERA in the form of a recommendation to the European Commission in July 2012.

Avoiding duplication of assessment processes

3.63 There are a number of assessment processes required under different laws:

(a) assessment of conformity with TSIs;
(b) assessment of safety certificates (for RUs) or safety authorisations (for IMs);
(c) independent assessment under the CSM on risk assessment.

3.64 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:

(a) A Notified Body can act as an assessment body (AB) under the CSM as long as it meets the criteria in the Regulation. So, if the significant change concerns sub-systems that are covered by TSIs, it is possible to appoint a NoBo that meets the criteria for independent assessment so that it can carry out the CSM assessment as well as the assessment of conformity with TSIs.

(b) If ORR has issued a safety certificate or authorisation, then the AB does not need to examine the general processes for risk assessment during the application of the CSM, but should look only at how the processes are applied for the specific change. However, if the AB finds that there are issues with the general processes for risk assessment these should be reported to the NSA and the proposer.

(c) If the proposer does not have a safety certificate or safety authorisation, then quality management systems may give the AB assurance about the general processes for change management and risk assessment within the proposer’s organisation.

(d) 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.

3.65 The regulation allows, but does not oblige, NSAs to act as an independent AB when a significant change also concerns:

(a) an authorisation for placing into service; or

(b) an update or revision of a safety certificate or safety authorisation.

3.66 ORR does not intend to act as an AB in these circumstances.

What is the role of the Assessment Body?

3.67 The AB checks that the CSM has been followed and also checks the results of the assessment. This could involve a sample or vertical audit to check:

- 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 para 3.21]
- 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;
- hazards and the associated safety measures are closed and validated.
3.68  ORR recommends that the AB 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. The AB must ensure that its involvement in these activities does not jeopardise its independence. The AB’s role in oversight does not remove the responsibility of the proposer for overall safety. **The proposer remains responsible for safety and takes the decision to implement the proposed change.**

3.69  At the conclusion of the assessment, a report is produced and this should support the proposer in taking the decision on the safety of the system. If the system also requires an authorisation to place into service, then the safety assessment report should also be submitted to the NSA with the technical file and other documentation. The NSA will take this into account in considering the authorisation.

3.70  Where an AB has delivered a safety assessment report, that report must be mutually recognised by any other AB, providing the system is used under the same conditions and equivalent risk acceptance criteria are applied.
4. Miscellaneous requirements of the Regulations

4.1 RUs and IMs should undertake periodic audits of the application of the Regulation as part of their safety management system arrangements.

4.2 RUs and IMs have to provide a safety report annually to ORR. The report should include:

- a summary of experience in applying the CSM process
- a summary report on the decisions related to significance of change.
Annex 1 Determining the significance of a change

1. When a proposed change has an impact on safety, the Regulation on the adoption of a common safety method on risk evaluation and assessment requires the proposer to decide, by expert judgement, the significance of the change based on stated criteria (Article 4.2).

2. These criteria are:
   a) 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;
   b) 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;
   c) complexity of the change;
   d) monitoring: the inability to monitor the implemented change throughout the system life-cycle and take appropriate interventions;
   e) reversibility: the inability to revert to the system before the change;
   f) 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.

3. The Regulation 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

4. It is possible to group and sequence the criteria in a way that assists their application.

   Additionality

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

6. 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 …).

7. One difficulty in examining a series of non-significant changes is determining what is meant by ‘recent’. Our interpretation of ‘recent changes’ is that they are changes that have not yet been implemented or are in the process of being implemented; WHEN the change is initiated is not relevant.

8. When a change has become fully implemented the proposer does not need to consider the change under additionality; in other words, once the change has become successfully embedded in the system. This would mean that a series of changes, each of which was introduced before the previous change had had time to take effect and been shown to be working successfully, would be caught by the additionality factor. However, once a change is established and working successfully,
the change can be regarded as fully implemented and does not need to be included in the consideration of additionality.

9. This would achieve the intention of the regulation (which refers to ‘recent’ safety-related modifications), whilst being practical and not imposing an arbitrary time limit.

**Novelty and complexity**

10. Novelty and complexity can be thought of as measures of the uncertainty of outcome – 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**

11. Failure consequence (or consequence of failure) is straightforward – 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**

12. Risk is usually understood to be likelihood x consequence, and 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**

13. 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.

14. 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, can you see what is going on and react in time?

15. In thinking about monitoring as a criterion, the question to be asked is therefore “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 you 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.

16. Reversibility in the sense of ‘revert[ing] to the system before the change’ will usually be of academic interest. 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. Reverting to the system before the change is one possible intervention, though one that is not usually available in the case of engineering change.
17. 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.
Flowchart illustrating proposed application of the criteria

A flowchart illustrating proposed application of the criteria along the lines set out above is shown below.
Judging significance

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.

An example of a possible matrix is shown below. Others (3 x 3 or 5 x 5 for example) are possible.

**Combining uncertainty of outcome and consequence of failure**

![Matrix diagram](image)

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Uncertainty</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = Insignificant</td>
<td>1 = Very low</td>
</tr>
<tr>
<td>2 = Marginal</td>
<td>2 = Low</td>
</tr>
<tr>
<td>3 = Critical</td>
<td>3 = Medium</td>
</tr>
<tr>
<td>4 = Catastrophic</td>
<td>4 = High</td>
</tr>
</tbody>
</table>

Legend:
- **Significant Change**
- **Apply Additional Criteria**
- **Non-Significant Change**
Annex 2 – Risk management process and independent assessment

![Risk management process and independent assessment diagram](image-url)
Annex 3 – Criteria which must be fulfilled by assessment bodies

1. The assessment body may not become involved either directly or as authorised representatives in the design, manufacture, construction, marketing, operation or maintenance of the system under assessment. This does not exclude the possibility of an exchange of technical information between that body and all the involved actors.

2. The assessment body must carry out the assessment with the greatest possible professional integrity and the greatest possible technical competence and must be free of any pressure and incentive, in particular of a financial type, which could affect their judgement or the results of their assessments, in particular from persons or groups of persons affected by the assessments.

3. The assessment body must possess the means required to perform adequately the technical and administrative tasks linked with the assessments; it shall also have access to the equipment needed for exceptional assessments.

4. The staff responsible for the assessments must possess:
   - proper technical and vocational training,
   - a satisfactory knowledge of the requirements relating to the assessments that they carry out and sufficient practice in those assessments,
   - the ability to draw up the safety assessment reports which constitute the formal conclusions of the assessments conducted.

5. The independence of the staff responsible for the independent assessments must be guaranteed. No official must be remunerated either on the basis of the number of assessments performed or of the results of those assessments.

6. Where the assessment body is external to the proposer’s organisation must have its civil liability ensured unless that liability is covered by the State under national law or unless the assessments are carried out directly by that Member State.

7. Where the assessment body is external to the proposer’s organisation its staff are bound by professional secrecy with regard to everything they learn in the performance of their duties (with the exception of the competent administrative authorities in the State where they perform those activities) in pursuance of this Regulation.

8. Proposals to amend the Regulation were made by the Commission in July 2012. These include a system of authorisation for assessment bodies for cross-border projects. The guidance will be updated when the new provisions have been agreed.
Annex 4 Guidance on organisational change

Purpose
1. This Annex provides high-level guidance on the application of the common safety method on risk evaluation and assessment (the CSM) when assessing significant organisational changes.

What is a significant organisational change?
2. It is a requirement of the CSM 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.

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.

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 has to be assessed individually in the context in which it is being applied.

5. The first consideration is whether the organisational change is within the scope of the CSM – could it impact on operating conditions of the railway system?

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.

7. If an organisational change does affect safety, one method for assessing whether a change is significant is offered in Annex 1 of this guidance.

Assessing the change
8. The CSM presents three ‘risk acceptance principles’ by which the hazards associated with a significant change can be analysed and evaluated:
   a) the application of codes of practice;
   b) a comparison with similar systems (reference systems); and
   c) an explicit risk estimation

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.
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.

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

(a) Definition of the extent of the change being made

(b) Preparation of disposition statements indicating where the safety responsibilities are transferred from one job description to the job description of the new role

(c) Checking that the new job roles specify the correct competency levels for the safety functions that have been transferred

(d) 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. A possible risk assessment approach for a significant organisational change is presented in the Appendix to this guidance.

(e) Recording and maintaining the outputs of the risk assessment in a hazard record

(f) Establishing the go-live criteria that need to be achieved before the organisational change is implemented

(g) Documentation of records relating to (a) to (g) above

**Risk Acceptance criteria**

12. The quantitative risk acceptance criteria defined in paragraph 2.5.4 of the CSM 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**

13. One of the main principles introduced by the CSM 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 any member state, i.e. once a significant change has been assessed and subject to an independent assessment by an Assessment Body, the change should be acceptable anywhere in the EU member states without additional assessment providing the same application conditions apply.

**Independent Assessment**

14. The CSM requires that all significant changes including organisational changes are independently assessed by an Assessment Body (AB), which produces a safety assessment report.

15. The role and requirements of an AB are described in the ORR guidance. The key to a successful independent assessment is getting the AB 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 AB has a good insight into the risk assessment process and the development of the hazard records. Early feedback from the AB can help in the development and refining of the risk assessment process being used.
16. The AB 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 AB 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
17. All stages of the CSM application should be documented and the hazard record established for use through the implementation of the change.

Risk assessment process
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.

19. This appendix provides an overview of an approach that could be used, based on the risk assessment work that was done for the review of the organisational changes associated with the establishment of the South West Trains / Network Rail Wessex Alliance.

20. The purpose of the workshops would be to identify whether the organisational changes could introduce safety concerns/issues and consider the measures that need to be put in place to control/mitigate any increase in risk. The extent of the workshops depends on the scale of the change, the number of people affected and their role in influencing safety.

21. The workshop(s) will enable individuals who will be affected by the change to better understand the objectives of the change and provide proactive input to the consideration of the safety implications of the change and any additional mitigating measures. The method should involve:

a) Clearly defining the change being made

b) Identifying who is affected by the change and needs to be consulted including:

   (ii) staff;
   (iii) representative bodies e.g. trades unions;
   (iv) interface organisations; and
   (v) other stakeholders

c) Facilitating the structured workshop(s) involving representatives of the groups that could be affected by the change.

d) The independent assessor should attend some or all or the workshops.

e) Development and maintenance a hazard record, including the measures to be taken to mitigate the risk from each identified hazard and the current status of the implementation of the control measures.

   a) The workshop(s) should be structured into topic areas that could be influenced by the organisational change rather than just a general brainstorming of the issues. The topic areas could include the potential influences on:

   a) The way the safety management system is implemented and managed;
b) The different risk areas such as train accident risk, station risk, on-train risk and infrastructure risk

c) Management of risk interfaces:
   (i) Incident/emergency management (on-track, at station, on-train)
   (ii) Degraded operations e.g. failed train and station safety e.g. Platform-train interface
   (iii) Safety reporting, safety meetings, risk reviews, accident investigations, etc

(d) Communications
(e) Safety decision making
(f) Operational strategy
(g) Maintenance strategy

Identification of safety concerns

22. Attendees should be asked to brainstorm the safety concerns they perceive against each of the topic areas in relation to the proposed organisational changes. The use of post-it notes can be useful here to ensure that each attendee has the opportunity to note down their own perceived issues. This will assist the facilitator in the collation of similar safety concerns into agreed safety concern statements.

23. Given the difficulty in assigning meaningful likelihood and consequence rankings to each safety concern for organisational changes, a simple high, medium and low vulnerability ranking can be considered such as:
   (a) High = Major concern – potential for significant degradation in safety
   (b) Medium = Some concern – potential for some degradation in safety
   (c) Low = Minimal concern – unlikely to significantly affect safety but should be reviewed

24. As each topic area is reviewed, participants should write their perceived safety concerns and associated vulnerability ranking onto individual post-it notes and place them on a flip chart/wall poster for the topic area divided into the high, medium and low vulnerability rankings.

25. Once all the post-it notes have been put on the relevant category poster the comments should be collated by the workshop facilitator and discussed by the group to produce agreed safety concern statements, including the overall perceived vulnerability ranking for each statement.

Identification of control measures

26. Having identified the safety concerns into agreed safety concern statements and their associated vulnerability rankings, the project team can develop a ranked hazard record. The relevant control/mitigation measures required to address each hazard can then be identified.

27. This can either be done in the workshop environment (if there are not too many safety concerns raised) or as a separate exercise by the project team and fed back to the participants for review.

28. The hazard record containing the agreed safety concern statements with their associated vulnerability rankings, control/mitigating actions, actions required, person(s) responsible for the
actions and the status of the actions can then be managed throughout the implementation phase to ensure the identified control/mitigation measures are put in place.

29. A requirement that the actions from the hazard record relevant to the development and start-up phases are completed should be part of the go-live criteria necessary to be addressed before the organisational change is implemented.