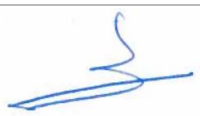
Guide

Issuing a safety certificate or safety authorisation

A guide for national safety authorities

	Elaborated by	*Validated by*	*Approved by*
Name	M. SCHITTEKATTE	H. DELSOIR	C. CARR
Position	Project Officer	Head of Sector	Head of Unit
Date	12/06/2015	12/06/2015	12/06/2015
Signature			

Document History

Version	*Date*	*Comments*
2.0	06/05/2015	Reformatting of the document, inclusion of inputs from the Working Party on the revision of CSMs for Conformity Assessment and CSM on Supervision.
2.1	12/06/2015	Final consultation with the Working Party on the revision of CSMs

Disclaimer:

The present document is a non-legally binding guidance of the European Railway Agency. It is without prejudice to the decision-making processes foreseen by the applicable EU legislation. Furthermore, a binding interpretation of EU law is the sole competence of the Court of Justice of the European Union.

Contents

1 Purpose and scope

The purpose of this guidance document is to address known issues faced by NSAs in relation to general principles underpinning the application for, the validity and update of safety certificates and safety authorisations. For ease of reading and as appropriate, the relevant EU legislation is referred to in the header of each main section. Frequently asked question(s) are also listed and an answer is proposed in the subsequent (sub-) sections.

This document also proposes a safety assessment process for NSAs to ensure a consistent approach to applications from Railway Undertakings and Infrastructure Managers, respectively for the granting of safety certificates and safety authorisations. Annex I of CSM on Conformity Assessment [4][5] requires a structured and auditable process which ensures that NSAs take similar decisions in similar circumstances and that there is a degree of assurance that the assessment process is undertaken in a similar way by all NSAs. The proposed safety assessment process should help the NSAs fulfil this requirement. It gives flexibility to the NSA to define their own organisational structure and associated roles and responsibilities. Similarly, the NSA is free to establish its own information management system consistent with the proposed safety assessment process (e.g. by defining a storage policy, including retention time and storage location, for records[1]). It is equally applicable to both the safety certification process and the safety authorisation process. For the purposes of this document reference to safety authorisation is made in brackets following the reference to safety certification for the reader's convenience.

The NSA is therefore invited to tailor the present safety assessment process to meet its specific (business) needs and objectives. It is not precluded from applying an audit framework as set out in ISO 19011[2] and/or applying on a voluntary basis, partly or wholly, the requirements for bodies providing audit and certification of management systems as set out in ISO 17021[3], provided that it does not impinge non-discriminatory principles (e.g. for new entrants to the rail market) and that it provides at least the same level of expected evidence. Timescales may also be added for each stage of the process with regards to the NSA's organisational and operational arrangements[4] (e.g. staffing, period of validity of safety certificate (or authorisation), internal procedures and/or objectives).

Model templates (e.g. application documents, standard format for safety authorisation and safety assessment forms) and specific case studies can be found in the annexes of the document.

[1] By definition, a record is a "document stating results achieved or providing evidence of activities performed" (ISO 9000:2005).

[2] ISO 19011 provides guidance on auditing management systems, including the principles of auditing, managing an audit programme and conducting management system audits, as well guidance on the evaluation of competence of individuals involved in the audit process.

[3] ISO 17021 applies to third party conformity assessment bodies verifying the conformance of an organisation's management system(s) to a standard (e.g. ISO 9001). The ISO 17021 standard requirements are more stringent than those applying to the NSA. For example, conformity assessment bodies have to implement, under a predefined timeframe, a two-stage (initial) audit, surveillance audits and a recertification audit prior to expiration of certification. They have also to draw up the audit plan in accordance with the relevant guidance provided in ISO 19011.

[4] This is beneficial in that the (lead) assessor knows the maximum allocated time per stage and helps plan resources / other work. For that purpose, ORR has developed an assessment timetable spreadsheet (ROGS timetable calculator) that allocates timings to each stage of the assessment process.

2 Background

Who can be granted a safety certificate or safety authorisation?

2.1 Definition of Railway Undertaking and Infrastructure Manager

Pursuant to Article 3 of Directive 2004/49/EC on safety on the Community's railways (Railway Safety Directive, hereinafter also "the RSD"), an Infrastructure Manager (IM) and a Railway Undertaking (RU) are defined as follows:

- '**Infrastructure Manager**' means any body or undertaking that is responsible in particular for establishing and maintaining railway infrastructure, or a part thereof, as defined in Article 3 of Directive 91/440/EEC, which may also include the management of infrastructure control and safety systems. The functions of the infrastructure manager on a network or part of a network may be allocated to different bodies or undertakings;
- '**Railway Undertaking**' means railway undertaking as defined in Directive 2001/14/EC, and any other public or private undertaking, the activity of which is to provide transport of goods and/or passengers by rail on the basis that the undertaking must ensure traction; this also includes undertakings which provide traction only.

Pursuant to Directive 2012/34/EU establishing a single European railway area and replacing Directive 2001/14/EC, the definition of Railway Undertaking is as follows:

- '**Railway Undertaking**' means any public or private undertaking licensed according to this Directive, the principal business of which is to provide services for the transport of goods and/or passengers by rail with a requirement that the undertaking ensure traction; this also includes undertakings which provide traction only;

There are several aspects to consider under this definition:

- Any undertaking that is licensed under the national provisions transposing Directive 2012/34/EU is and shall be considered as RU.
- As regards other undertakings which are not licensed under the national provisions transposing Directive 2012/34/EU, there are two aspects to consider to decide whether an undertaking is a RU or not under the scope of the RSD[5]:
  - The activity of the undertaking is to provide transport of goods and/or passengers by rail on the basis that the undertaking must ensure traction;
  - The undertakings provide traction only.

The above definitions clearly make a distinction between the railway companies based on their activities:

- The IM is responsible for establishing and maintaining the railway infrastructure which may include the management of infrastructure control and safety systems.
- The RU provides transport of goods and/or passengers by rail with the requirement that it must also ensure traction. Those companies which provide only traction are also considered as RUs.

[5] *The scope of Directive 2012/34/EU and Directive 2004/49/EC is different. Therefore, it is possible to have RUs not required to have a licence under Article 2 of Directive 2012/34/EU whilst they are required to have a safety certificate under Article 2 of Directive 2004/49/EC. The safety on the whole rail system shall be respected and safety requirements shall be applied by any company, irrespective of whether provision of transport of goods and/or passengers is a principal business of the company or not, that uses the rail system not excluded under Article 2(2) of Directive 2004/49/EC. In addition, Member States may exclude certain RUs from the obligations of having a licence under Directive 2012/34/EU (e.g. undertakings which only operate rail passenger services on local and regional stand-alone railway infrastructure); however, these RUs may not be excluded from their safety obligations according to Directive 2004/49/EC.*

2.2 Legal requirements

The requirements of the RSD, including the obligation for safety certificate or safety authorisation, are valid only for those companies which fall under its scope.

If a company is considered as an RU either under the RSD or Directive 2012/34/EU (i.e. it provides transport of goods and/or passengers by rail with traction or only traction), it shall have a safety certificate (Part A and Part B) according to the RSD to be authorised to carry out its activities and to be granted access to an infrastructure.

Those RUs whose principal business is to transport goods and/or passengers shall have a licence according to Directive 2012/34/EU. For these RUs a valid licence[6] and a safety certificate are the conditions to be granted access to the railway infrastructure.

If a company is considered as an IM (i.e. it establishes and maintains railway infrastructure which may include the management of infrastructure control and safety systems), it shall have a safety authorisation according to the RSD to be authorised to carry out its maintenance activities on an infrastructure.

It is important to note that first it shall be decided whether a company is considered a RU or IM (or both[7]) based on its activities, and then the appropriate applications for the required authority documents (licence, safety certificate or safety authorisation) shall be launched.

To ensure that safety risks associated to railway activities of Railway Undertakings and Infrastructure Managers are controlled, no movement of trains or rakes of vehicles can be made on the rail network under the responsibility of an Infrastructure Manager if the risks associated to this movement is not controlled through the SMS of a Railway Undertaking or of an Infrastructure Manager. This principle derives from Article 9(2) of RSD. Therefore, no movement of trains or rakes of vehicles can be made on the rail network under the responsibility of an Infrastructure Manager if they are not covered by a safety certificate or a safety authorisation.

It means that those movements can only be done by Railway Undertakings or Infrastructure Managers having valid safety certificates or safety authorisations or by any other organisation acting as subcontractor for those Railway Undertakings or Infrastructure Managers.

Therefore, the following basic principles apply:

- No movement of vehicles can be made on a railway network if associated risks are not controlled by means of the Safety Management System (SMS) of either an RU or an IM;
- Safety certification/authorisation provides assurance that SMS of the RU/IM controls the safety risks;
- No movement of vehicles can be made if not covered by safety certificate or safety authorisation.

2.3 Infrastructure Manager's capacity to operate vehicles on its own network

IMs may need to use vehicles to transport materials for construction or for infrastructure maintenance activities or to perform infrastructure maintenance. For that purposes, either the IM is responsible for the train movements (e.g. use of yellow machines) on its own infrastructure or it may (partly or wholly) outsource the train operations to other companies (such as RUs) under contractual arrangements (See also section 3.1.3).

The assessment of the IM's capacity to operate vehicles on its own network (directly or via subcontractors) may be either part of its assessment for a safety authorisation, providing it is within the limit of their activities

[6] *Pursuant to the definition of Railway Undertaking provided for in Directive 2012/34/EU, a licence should not be required from a company whose principal business is not to transport goods and/or passengers.*
[7] *In accordance with requirements set out in Section 2 of Directive 2012/34/EU.*

and they are not providing additional services such as transport of goods and/or passengers, or be subject to a new assessment for a safety certificate.

In the first case, in addition to the requirements and criteria of the CSM Regulation for Conformity Assessment 1169/2010/EU, the NSA issuing the safety authorisation should check the criteria in Annex II of the CSM Regulation for Conformity Assessment 1158/2010/EU that are specific to maintenance of rolling stock (e.g. criterion B.2). Particular attention should also be paid to the criteria relating to the management of contractors and suppliers (i.e. criteria B, C).

The relevant criteria in Annex II of the CSM Regulation for Conformity Assessment 1158/2010/EU shall be applied by the NSA, irrespective of how the business is organised. However, the NSA is not allowed to issue "limited[8]" safety certificates for the IM (that can still operate under its safety authorisation) or its subcontractors (that can operate under their own safety certificate or under the IM's safety authorisation).

[8] *Partial compliance with Regulation (EU) n°1158/2010.*

3 Application for a safety certificate or safety authorisation

When and by whom should a Part A and a Part B safety certificate be issued?

What are the parts of the safety management system (SMS) related to the Part A and Part B safety certificates?

If a RU decides to operate a new (part of) line, shall the NSA issue a new Part B safety certificate?

Which information should be included in the application form for safety certificate or safety authorisation?

"The safety certificate shall comprise […] certification confirming acceptance of the provisions adopted by the railway undertaking to meet specific requirements necessary for the safe operation of the relevant network. The requirements may include application of TSIs and national safety rules, acceptance of staff's certificates and authorisation to place in service the rolling stock used by the railway undertaking. The certification shall be based on documentation submitted by the railway undertaking as described in Annex IV."

Art. 10(2)(b) of Directive 2004/49/EC (Railway Safety Directive)

"The safety authority in the Member State where the railway undertaking first establishes its operation shall grant the certification in accordance with paragraph 2.

The certification granted in accordance with paragraph 2 must specify the type and extent of the railway operations covered. The certification granted in accordance with paragraph 2(a) shall be valid throughout the Community for equivalent rail transport operations."

Art. 10(3) of Directive 2004/49/EC (Railway Safety Directive)

"The safety authority in the Member State in which the railway undertaking is planning to operate additional rail transport services shall grant the additional national certification necessary in accordance with paragraph 2(b)."

Art. 10(4) of Directive 2004/49/EC (Railway Safety Directive)

3.1 Scope

RU and IM must establish a SMS and make it effective to ensure the safe operation of the railways, each one having the safety responsibility for its part of the system and its own operations.

Once, the company is considered as an RU or an IM and has established its SMS, it shall hold respectively a safety certificate or a safety authorisation in accordance with the RSD.

The scope of a Part A safety certificate covers all elements of the SMS whereas the scope of a Part B safety certificate only covers the following network specific elements defined in Annex III of CSM Regulation for Conformity Assessment 1158/2010/EU:

- Competence management system;
- Compliance with applicable network specific national rules;
- Asset management (rolling stock).

As follows, if an RU provides rail transport services only in one Member State, then the company shall have a Part A and a Part B safety certificate granted by the NSA where the RU provides its services.

If an RU wishes to operate in MS other than the one where it first established its operation and was granted its Part A safety certificate, the same RU shall apply for a Part B safety certificate in the other Member State.

The NSA of the other Member State may not and shall not require the RU to apply again for Part A safety certificate.

If the NSA of the other Member State has any issues or doubts concerning the Part A safety certificate of the RU, the NSA shall cooperate with the NSA that issued the Part A safety certificate (Cf. Annex I of CSM Regulation on Conformity Assessment 1158/2010/EU). The NSA issuing the Part A safety certificate should be informed of the issue of the additional Part B safety certificate because starting operation in another Member State may in some cases be an operational/organisational change that the RU should assess (significance of the change) and where necessary proceed with the application of CSM Regulation on risk evaluation and assessment 402/2013/EU. Following it, the identified risk control measure(s) may induce a change of the SMS arrangements resulting in an update of the Part A safety certificate (see also section 5).

If an RU decides to establish a new company in another Member State to provide services in that MS, it is entirely up to the company to decide so. However, the new company shall follow all the requirements laid upon RUs in the RSD, i.e. apply for a licence, if needed[9], establish its own SMS and apply for both Part A and Part B safety certificates in the other Member State.

It is not foreseen in the RSD that in this case companies could rely on each other's licences, safety certificates and SMS.

3.1.1 Specific considerations for the granting of Part A safety certificate

Part A safety certificate certifies the acceptance of the RU's SMS and shall be granted by the NSA of the Member State where the RU first establishes its operation (Article 10(3) of RSD).

A company shall have only one Part A safety certificate which shall be given by the NSA where the company establishes its operation for the first time. Such Part A safety certificate shall be valid throughout the European Union for equivalent rail transport operations.

If the same company extends its operation to another Member State, without establishing a new company in that Member State, the company shall not apply for a new Part A safety certificate. That condition is in line with the principle of free movement of services set out in Article 56 of the Treaty on the Functioning of the European Union: *"Within the framework of the provisions set out below, restrictions on freedom to provide services within the Union shall be prohibited in respect of nationals of Member States who are established in a Member State other than that of the person for whom the services are intended."*

3.1.2 Specific considerations for the granting of Part B safety certificate

Part B safety certificate certify the acceptance of the RU's provisions to meet the networks' specific requirements and shall be granted by the NSA of the Member State where the RU first establishes its operation (Cf. Article 10(3) of RSD) and by any other NSA where the RU is planning to operate additional rail transport services (Cf. Article 10(4) of RSD).

NSA's assessment of an application for a Part B safety certificate shall only apply to a RU's capability to comply with the requirements needed to operate on the specific network for which it is seeking a certificate. The assessment of the Part B should link back to the requirements in the Part A. For example, any rules for competence requirements should link to the processes set out for compliance with criteria N in the Part A.

The RSD stipulates in its Article 10(2)(b), 10(3) and 10(4) that a Part B safety certificate is required when entering a rail network. In other words:

[9] *Directive 2012/34/EU establishes the principles and procedures for train path allocation. It states that RUs shall be granted, under equitable, non-discriminatory and transparent conditions, the right to access to the railway infrastructure in all MS (Article 10). Moreover, IMs shall supply to all RUs in a non-discriminatory manner the minimum access package (Article 13). All basic principles, obligations, rights, etc. set out in this Directive for RUs are applicable only to those undertakings which are licensed in line with the corresponding definition in Article 3(1).*

a) For domestic operations, the RU should only apply for a Part B safety certificate in its own Member State.

b) For international operations, in addition to its domestic Part B safety certificate, the RU should also apply for a Part B safety certificate in the Member State(s) where it plans its operation(s). However, the assessment of the application for a Part B safety certificate by the neighbouring Member State(s) should be proportionate to the risks incurred and the type and extent of the operation.

If the RU decides to operate on a new line or even on new parts of a same line, the existing Part B safety certificate shall be updated with the new line condition. In any case, the newly updated Part B safety certificate always replaces the previous one (that is no more active in ERADIS database). Therefore, the latest Part B certificate should reflect all line conditions (i.e. all conditions since the first issued Part B safety certificate). However, the reassessment should be proportionate to the change.

The geographical scope of Part B safety certificate should cover the railway network[10] of a Member State or only a defined part[11] thereof (Article 10 of RSD) where the RU operates. The RU may operate on the infrastructure of a number of different IMs. The nature of the infrastructure managed by one IM is detailed in its network statement (Articles 3(26) and 27 of Directive 2012/34/EU). In case the network of a Member State is managed by more than one IM, the network statements developed by the IMs give detailed information on the nature of the whole network of the Member State and the RU should then be permitted to have just one Part B certificate. Therefore, it can be concluded that the detailed information on the nature of the infrastructure falling under a Part B safety certificate is specified in the relevant network statement(s).

A train will not be considered to be a cross-border service if all the vehicles of the train crossing the state border cross it only to the 'frontier' location(s), i.e. any location(s) designated as the 'frontier' in the network statement of an infrastructure manager. The arrangements and cooperation agreements between IMs of neighbouring Member States stated in their respective network statement should ensure cross-border operations under "similar network characteristics" and "similar operating rules". Therefore, a new Part B safety certificate **might not be required** for those RUs operating until the frontier location(s) in the other Member State(s) (e.g. first station located beyond the state border). In such cases, the acceptance of the RU's provisions to meet the network specific requirements (between the state border and the frontier location(s)) could be part of the domestic Part B safety certificate granted by the NSA of the Member State where the RU is registered to avoid duplicating work and additional procedural cost. However, the practicality of such an arrangement is left to the decision of the neighbouring Member States, which have to agree beforehand on the definition of 'frontier' location(s), as it might be subordinated to the compliance check with the different national rules applying in each Member State, national laws in force, bilateral agreement, treaty etc. In any case, the neighbouring NSAs shall cooperate together during the assessment and post-award supervision to oversee the specific case of the 'frontier' location(s).

In absence of special arrangements between Member States, a part B safety certificate is necessary as soon as the state border (or Concession Boundary in the case of the Channel Tunnel Concession Area) is crossed. The assessment of the application for a Part B safety certificate by the neighbouring Member State(s) should be proportionate to the area of operation (e.g. operation until the border station) in addition to the risks incurred and the type and extent of the operation.

3.1.3 Cooperation regimes between RUs

The RU is responsible to ensure the safe running of the train by coordinating and managing the train operations.

---

[10] The railway network is defined as "the entire railway infrastructure managed by an infrastructure manager" (Article 3(25) of Directive 2012/34/EU).
[11] It is therefore necessary to specify clearly all the lines where services (passenger, freight or shunting only) are intended to be operated (3.16 of Regulation 653/2007/EC) if the RU does not wish to operate on the whole network.

Contractual agreements (usually consisting of framework agreement, special agreements and annexes) constitute the grounding for effective cooperation between different RUs, be it “new entrants” or “incumbents”, and have to comply with the provisions of the European and national legislation and any other applicable requirements.

Therefore the RU shall control the risks of its operations, including cooperation with partners and use of contractors. The NSA shall then supervise that the RU fulfils its legal obligations in a transparent and diligent manner. RUs cannot outsource their safety responsibility for coordinating and managing the safe running of the train, which is not detrimental to the existence of cooperation regimes between RUs (See also Annex 3 case 3). The basic principles set out in section 2.2 also apply to cooperation between RUs. The RU responsible to ensure the safe running of the train must be clearly identified in any type of agreements between involved parties and must hold a safety certificate. Either this RU directly manage the resources (personnel, vehicles) through its SMS or it may decide to subcontract (partly or wholly) the use of the resources (e.g. leasing of vehicles, hiring of train drivers) to another party. In the latter case, the RU has still the responsibility to control the risks relating to the use of (sub)contractors through its SMS (See CSM Regulation on monitoring 1078/2012/EU) and therefore, has to check that these resources comply with the legal and other applicable safety requirements (e.g. vehicles in a safe state of running, route compatibility, staff training, train drivers with a valid licence and certificate for a specific route). A safety certificate delivered by a NSA (and supervised accordingly) to the contracting party (i.e. the partner or subcontractor) can provide sufficient assurance to the RU responsible for the safe operation that the SMS arrangements meet the relevant requirements. The contractual arrangements should include the transfer of information relevant to safety (e.g. previous rest time of the train drivers) between the contracting parties.

The principles underpinning cooperation between RUs remain the same irrespective of cooperation regimes, i.e. partnership or subcontracting (partly or wholly) railway activities in domestic or cross-border operations. However, the nature and extent of measures to be implemented by RUs and the extent to which the NSA has to supervise these cooperation arrangements are proportionate to the degree of cooperation between RUs.

For example, cross-border cooperation between RUs (i.e. use of external vehicles and/or staff) is likely to require more controls than any other cooperation regimes because the operation is handed over to another RU with different languages and operating rules for rolling stock that may apply from one Member State to another. In contrast, hiring external train drivers or vehicles only would obviously require less monitoring and NSA supervisory activities.

The identification of the cooperation regimes between RUs, the definition of responsibilities (i.e. who is responsible for the safe running of the train) and the nature of the contractual arrangements ruling it shall be documented in the SMS and then, be made accessible to the competent NSA(s) (See also Annex 4).

Without prejudice to the previous conditions, any arrangement made between companies regarding other aspects of the train operation (e.g. commercial aspects, request or use of train path) must not have a negative effect on the obligations of the RU to have a safety certificate.

3.1.4 Siding operations

In this document, ‘siding’ means railway infrastructure connected to the railway network under the responsibility of an IM (i.e. the infrastructure part of the rail system falling under the scope of RSD). Siding is or is not part of this rail network.

Activities performed on sidings are industrial activities interfaced with railway and railway activities such as composition, preparation and movement of rakes of vehicles that can be trains or will be used in trains. It includes coupling different vehicles to form rakes of vehicles or trains and moving them.

Those sidings may be (but not limited to):

- Industrial areas or plants where industrial activities of loading /unloading of freight wagons are performed;
- Intermodal terminals;
- Infrastructures used for services on passenger vehicles such as cleaning or light maintenance;
- Infrastructure belonging to and managed by a maintenance workshop for railway vehicles;
- Infrastructure used to park railway vehicles between operations.

The activities performed on sidings are performed by a "siding operator".

In general the siding operator is not a RU or an IM but a service provider (e.g. for cleaning passenger vehicles) or an industrial organisation (e.g. a chemical plant loading/unloading tank wagons)

Nevertheless, the siding operator may also be a RU or an IM.

Case 1: The siding operator is a Railway Undertaking

This RU controls, through its SMS, the risks associated with its railway operations on its infrastructure (the siding) and on the railway network under the responsibility of the IM. This control of risks includes risks associated with damages on vehicles caused by all activities performed in the siding including also composition, preparation and running of trains.

The RU controls the risks associated to occupational health and safety through its health and safety management system in place according to international and national legislation.

In practice it is sometimes difficult to determine the responsible Railway Undertaking; for example a RU "X" arrives as a train (driver and locomotive are hired) and a RU "Y" then takes it over as the following train (driver and locomotive are hired) and in the meantime siding operations need to be carried out. In this case, the above safety principle applies. There are shared interface risks that must be considered in the RU "Y"'s SMS (e.g. damage to vehicle caused by siding operations such as loading). In addition, the transfer of information about the vehicles from the RU "X" to the RU "Y" directly or via the siding operator should also be considered. This would include the assurance that the vehicle is in a safe state of running when RU "X" transferred it to the siding operator. The RU remains fully accountable for the control of risks inherent in the maintenance activities on the vehicle (even if this control is subcontracted to a third party).

Case 2: The siding operator is not a Railway Undertaking

The siding operator controls the risks associated with occupational health and safety through its SMS. It includes the health and safety obligations related to external workers in particular those of RUs, for instance when drivers enter the siding with a train. In parallel, the Railway Undertaking controls the risks associated with occupational health and safety through its health and safety management system in place according to international and national legislation.

4 subcases can be considered:

- **Subcase 2.1** when the siding operator is the IM.
- **Subcases 2.2 and 2.3** when siding operator, not being IM, performs activities only on its own infrastructure but not on the rail network under the responsibility of the IM.
- **Subcase 2.4** includes railway operations performed by siding operator (not being IM) on the rail network under the responsibility of the IM.

Subcase 2.1: Whatever activities on the siding are shared between RU(s) and IM (or any organisation acting of its behalf), each RU must be informed of all safety events thattake place during the activities of the IM through contractual arrangements. That includes damages, accidents and incidents on vehicles.

Those contractual arrangements are managed respectively through the SMS of each RU and the SMS of the IM.

Through its SMS, the RU controls the risks associated with its own operations in relation to this information received.

Subcase 2.2: Train composition and preparation is made by the RU (coupling, preparation) on the siding infrastructure. The RU must be informed of all (safety) events that take place during the activities of the siding operator (e.g. loading or cleaning) through contractual arrangements. That includes damages, accidents and incidents on vehicles.

Those contractual arrangements are managed by the SMS of the RU.

Through its SMS, the RU controls the risks associated to its own following operations in relation to this information received.

Subcase 2.3: Train composition is fully/partially performed by the siding operator or by an organisation working on behalf of the siding operator.

After train is composed, it is transferred to one Railway Undertaking.

Likewise subcase 2.2, the RU must be informed of all (safety) events that take place during the activities of the siding operator (e.g. loading or cleaning) and during train composition through contractual arrangements. That includes damages, accidents and incidents on vehicles.

Those contractual arrangements are managed by the SMS of the RU.

Through its SMS, the RU controls the risks associated to its own operations in relation to the information received.

Subcase 2.4: This subcase complements subcase 2.3. Therefore, only additional duty of RU is introduced hereafter.

The siding operator runs trains or move rakes of vehicles from its own rail infrastructure onto the railway network under the responsibility of an IM.

For example:

- Move the train or rakes of vehicles from a service yard to the platforms of a passenger station or to a parking yard attached to a passenger station;
- Move the train or rakes of vehicles from an industrial plant to an interchange point (exchange siding) attached to a freight station.

The siding operator is neither an RU nor an IM but the first principle here above must be respected.

Therefore those operations performed on the network of an IM must be covered by a safety certificate or a safety authorisation.

Imposing on a siding operator the need to have a safety certificate is in many cases nonsense from an economic point of view.

The two remaining solutions are that the railway operations made by the siding operator on the rail network under the responsibility of an IM are covered by the safety certificate of a RU or by the safety authorisation of the IM. This means that the RU or the IM must control the risks associated with the operations performed by the siding operator through the arrangements for the management of subcontractors in their SMS.

In all cases, the RUs and the IM must accurately describe the scope of all their railway operations and of their other activities interfaced with railway operations to make the supervision of the SMS by NSAs effective. The capability of RUs and IMs to describe clearly and completely their operations and their other activities interfaced with railway operations is essential for ensuring the effectiveness of the SMS and the effectiveness of NSA supervision.

The contractual arrangements in all above subcases must include clearly (but are not limited to):

- What has to be done by each contracting party;
- The expected quality of the outputs (services);
- Assignment of roles and responsibilities;
- What, when and how information will be exchanged between the contractual parties. Information includes reporting on events as described in all subcases above and particularities of the infrastructure of the siding such as speed limits, weight limits or gradient conditions;
- Competence requirements;
- Health and safety requirements (deriving from risk assessment, national requirements, etc.).

3.2 Forms

Applications for Part A and/or Part B certificates shall be submitted in accordance with Articles 10 and 12 of Directive 2004/49/EC and shall use the form set out in Annex III to Regulation 653/2007/EC. Part A and Part B safety certificates shall use the standard format respectively set out in Annex VI to Regulation 445/2011/EU (replacing Annex I of Regulation 653/2007/EC) and in Annex II to Regulation 653/2007/EC.

Applications for safety authorisation shall be submitted in accordance with Articles 11 and 12 of Directive 2004/49/EC and may use the form set out in Annex 1 to this document. Safety authorisations may also use the standard format set out in Annex 2 to this document.

Guidelines on information to be entered into the application form for safety certificates Part A and Part B are also provided for in the Annex III of Regulation 653/2007/EC. As far as practicable, unless stated otherwise in the present document, the same guidelines may also apply for safety authorisation. For example, the numbering system introduced in Annex IV of Regulation 653/2007/EC already identifies a specific code (i.e. 2 1) for safety authorisation.

The RU/IM shall inform the relevant NSA to which it applies for a safety certificate/authorisation of the following particular conditions:

- Whether the RU/IM acts as ECM. Therefore, the safety certificate/authorisation shall reflect the status of the ECM certification, including outsourced maintenance functions (or parts of them) if any;
- Whether the IM operates traffic for construction or maintenance for its own needs (see section 2.3).

When granting the safety certificate/authorisation, it is recommended that the NSA identifies those conditions in the 'additional information' field of the safety certificate or safety authorisation.

4 Validity of safety certificates

Can the validity of Part B safety certificate be extended beyond the validity of Part A safety certificate?

"In order to be granted access to the railway infrastructure, a railway undertaking must hold a safety certificate... The safety certificate may cover the whole railway network of a Member State or only a defined part thereof. […]"

Art. 10(1) of Directive 2004/49/EC (Railway Safety Directive)

"The safety authority in the Member State where the railway undertaking first establishes its operation shall grant the certification in accordance with paragraph 2. […] The certification granted in accordance with paragraph 2(a) shall be valid throughout the Community for equivalent rail transport operations.

The safety authority in the Member State in which the railway undertaking is planning to operate additional rail transport services shall grant the additional national certification necessary in accordance with paragraph 2(b)."

Art. 10(3-4) of Directive 2004/49/EC (Railway Safety Directive)

"The safety certificate shall be renewed upon application by the railway undertaking at intervals not exceeding five years. It shall be wholly or partly updated whenever the type or extent of the operation is substantially altered.

The holder of the safety certificate shall without delay inform the competent safety authority of all major changes in the conditions of the relevant part of the safety certificate. It shall furthermore notify the competent safety authority whenever new categories of staff or new types of rolling stock are introduced.

The safety authority may require that the relevant part of the safety certificate be revised following substantial changes in the safety regulatory framework. If the safety authority finds that the holder of the safety certificate no longer satisfies the conditions for a certification which it has issued, it shall revoke part (a) and/or (b) of the certificate, giving reasons for its decision. The safety authority that has revoked an additional national certification granted in accordance with paragraph 4 shall promptly inform the safety authority that granted the certification under paragraph 2(a) of its decision. Similarly, a safety authority must revoke a safety certificate if it is apparent that the holder of the safety certificate has not used it as intended in the year following its issue."

Art. 10(5) of Directive 2004/49/EC (Railway Safety Directive)

"The safety authority shall inform the Agency within one month of the safety certificates referred to in paragraph 2(a) that have been issued, renewed, amended or revoked. It shall state the name and address of the railway undertaking, the issue date, scope and validity of the safety certificate and, in case of revocation, the reasons for its decision."

Art. 10(6) of Directive 2004/49/EC (Railway Safety Directive)

4.1 General context

The RSD establishes the concept of one safety certificate necessary for a RU to be granted access to the railway infrastructure and makes a difference between the geographical validity between its constituting parts. Indeed, a Part A is valid in the whole EU while the relevant Part B is valid only on a specific network in a Member State.

The RSD makes no explicit difference between the validity in time between the two parts of the safety certificate as all the conditions for renewal, update and revocation set out in the RSD are relevant for both parts of the safety certificate.

The general principles of the RSD are reflected in the whole application procedure and the common format for safety certificate and the guidelines as described in Regulation 653/2007/EC.

4.2 Legal requirements

A RU shall have a valid safety certificate of which both parts are valid both in time and geographically. The geographical validity is relevant only for Part B.

As follows, the Part A safety certificate is valid in all EU Member States, and if the RU wishes to operate in other countries than the one in which it first established its operation, then the RU needs to obtain a Part B safety certificate for that network.

If the Part A of the safety certificate is affected by renewal, update, suspension or revocation, the relevant Part(s) B of the safety certificate should also be considered by the NSA issuing it.

For example, if the Part A safety certificate is up for renewal, then the complete safety certificate with all its parts (i.e. both Part A and Part(s) B) is subject to renewal. This approach can also be justified by the fact that in the course of the application process, it seems clear that the Part B safety certificate is issued based on, amongst others, the Part A safety certificate which includes the SMS processes against which the Part B was assessed.

Even the change of the numbering of the Part A safety certificate (if nothing changes in the conditions for issuing the new Part A safety certificate) should trigger at least a modification of the Part B safety certificate. The same may also apply to Part B safety certificate the change of which may trigger some changes in the Part A safety certificate. However, the level of assessment needed should be proportionate to the change and is up to the issuing NSA to decide on this. Therefore, co-operation and a quick and efficient system of exchange of information amongst the NSAs concerned is essential in case of renewal, update, suspension or revocation of one part of the safety certificate. However, it is also necessary to consider the administrative burden to the RU dealing with applications and following dialogue with several NSAs at the same time.

The standard formats for each part of the safety certificate allow for the possibility for each part to have different validity periods.

However, whenever either part of the safety certificate has been updated or renewed, the NSA issuing the other part of the safety certificate shall be informed and make a decision whether an assessment is necessary or not and which amendments to such other part of the safety certificate may be required.

Similarly, whenever either part of the safety certificate has been suspended or revoked, the NSA issuing the other part of the safety certificate shall be informed to take the appropriate actions. In case the NSA grants one part of a safety certificate which has a different validity period from the other part, the RU can carry out its activities and be granted access only if both parts of the safety certificate are valid both in time and geographically[12]. Without prejudice to the responsibility of the RU to have valid safety certificate (both Part A and Part B), the NSA issuing the Part B shall check the validity of the relevant Part A and make sure that the Part B will always be linked to a valid Part A.

Update (or amendment) of Part A or Part B safety certificate(s) should not lead to the extension of their validity period. Only renewal should allow for setting a new validity period. If Part A and Part B(s) have different validity periods, the NSA may always encourage the applicant to submit simultaneously its application for the renewal of all parts of its safety certificate. The NSA may also change the validity periods of safety certificates by the renewal of their relevant part(s) in consultation with applicants.

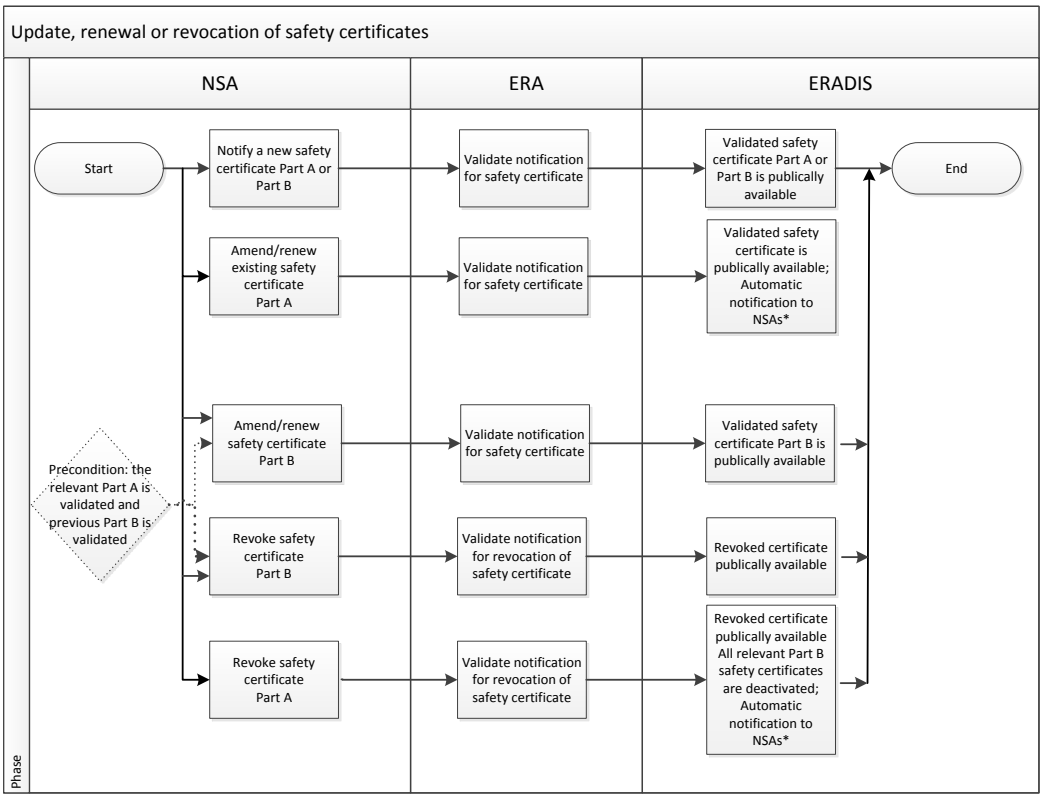
[12] *The geographical validity is relevant only for Part B safety certificates. The Part A safety certificate is valid in all MS and if the RU wishes to operate in other countries than the one in which it first established its operation, then the RU needs to obtain a Part B safety certificate for that network.*

4.3 ERADIS database

The ERADIS database provides public access (among other documents) to the safety certificates issued in accordance with Article 10 of RSD. The safety certificate confirms the acceptance of the provisions adopted by the RU to meet specific requirements necessary for the safe operation on the relevant network and applicable national legislation. All safety certificates issued, renewed, amended or revoked by the NSAs must be notified to the Agency via the ERADIS database.

The behaviour of the system is illustrated in the following flowchart:

- In case of renewal or amendment of Part A safety certificate, during the transition phase (i.e. the notification of a renewed or amended Part A safety certificate is not yet validated in ERADIS database), the former Part A safety certificate and relevant Part B safety certificate(s) should remain valid until its validity end date. Note that Part B safety certificates refer to the unique European Identification Number (EIN) of the relevant Part A safety certificate. Therefore the NSA must renew, amend or issue a new Part B safety certificate to be linked to the renewed or amended Part A safety certificate. Part B remains valid until its own validity end date. Once Part A expires, if Part B had longer validity period, it will not expire but will be still shown as valid until the validity end date. However, RUs should have both Parts of the safety certificate valid in order to perform their activities. The validity start date of a safety certificate is independent from the duration of the validation process of the notification in ERADIS database. The RU can start its operation from the validity start date of the safety certificate issued by the NSA.
- In case of revocation of Part A safety certificate, all related Part B safety certificates become inactive since a Part B cannot be valid without any related valid Part A.
- In case of revocation of Part B safety certificate(s), the relevant Part A safety certificate remains valid and active.



(*) The notification does not only target the NSA amending/renewing or revoking the Part A safety certificate but also the other NSAs issuing the relevant Part B safety certificate(s).

4.4 Good practices

In case the Part B is granted close to the end of validity of the relevant Part A, there would be a need to re-issue a new Part B within a short period of time which may create administrative burden and possibly additional cost of renewal. Similarly, it often occurs that international RUs start their operations on a limited number of lines and apply after a few years for extending their services to more lines. In any case new Part B safety certificates should be re-issued as soon as the relevant Part A is renewed. The NSA should have a proportionate approach to the Part B reassessment.

This issue is not related specifically to ERADIS but to the certification process itself and to mutual cooperation amongst NSAs, which should be strengthened in order to deal properly with Part B safety certificates issued to international RUs (See section 4.2).

The following best practice should be observed by the NSAs when issuing the Part A safety certificates:

- The validity of the new safety certificate should not start prior to the end validity of the original safety certificate;
- New safety certificates should be promptly notified to ERA and when applicable, no later than the end of validity of the previous safety certificates;
- The validity period of new safety certificates is recommended to be granted as far as possible for five years[13]. Member States may voluntarily reduce the validity period of safety certificates to enforce their decisions (e.g. implementation of a corrective action plan within an agreed time plan). In such case, it is of prime importance that all NSAs strengthen even more their mutual co-operation in order to deal properly with Part B safety certificates issued to international RUs.
- In case of update/renewal of a Part A safety certificate, the applicants are advised to apply as far as reasonably practicable for both Part A and Part B safety certificates at the same time. However, the NSA shall ensure that the Part A safety certificate is granted first or that both certificates are granted together as provided for in Regulation 653/2007/EC (Cf. Annex I(6) of CSM Regulation for Conformity Assessment 1158/2010/EU). As mentioned above, in such cases, it is of prime importance that all NSAs strengthen even more their mutual co-operation in order to avoid situations where the (conformity) assessment for Part B safety certificate(s) only starts after the granting of the updated/renewed Part A safety certificate and therefore, the railway company operates without valid Part B safety certificate(s). The update/renewal of Part B safety certificate(s) should be proportionate to the nature and importance of the changes (See also section 5).

[13] *Depending on the transposition of Article 10(5) of Directive 2004/49/EC in each Member State, the validity period of safety certificates might be shorter than five years.*

5 Update of safety certificates or safety authorisations

When shall a safety certificate or safety authorisation be updated?

"Infrastructure managers and railway undertakings shall establish their safety management systems to ensure" among others "that the railway system… is in conformity with the national safety rules… and with safety requirements laid down in the TSIs…"

Art. 9(1) of Directive 2004/49/EC (Railway Safety Directive)

"The safety management system shall meet the requirements and contain the elements laid down in Annex III, adapted to the character, extent and other conditions of the activity pursued. It shall ensure the control of all risks associated with the activity of the infrastructure manager or railway undertaking, including the supply of maintenance and material and the use of contractors".

Art. 9(2) of Directive 2004/49/EC (Railway Safety Directive)

"The safety certificate shall be renewed upon application by the railway undertaking at intervals not exceeding five years. ***It shall be wholly or partly updated whenever the type or extent of the operation is substantially altered****.*

The holder of the safety certificate shall without delay inform the competent safety authority of all major changes in the conditions of the relevant part of the safety certificate*. It shall furthermore notify the competent safety authority whenever new categories of staff or new types of rolling stock are introduced****.*

The safety authority may require that the relevant part of the safety certificate be revised following substantial changes in the safety regulatory framework*. […]"*

Art. 10(5) of Directive 2004/49/EC (Railway Safety Directive)

"The safety authorisation shall be renewed upon application by the infrastructure manager at intervals not exceeding five years. ***It shall be wholly or partly updated whenever substantial changes are made to the infrastructure, signalling or energy supply or to the principles of its operation and maintenance. The holder of the safety authorisation shall without delay inform the safety authority of all such changes****.*

The safety authority may require that the safety authorisation be revised following substantial changes to the safety regulatory framework*. […]"*

Art. 11(2) of Directive 2004/49/EC (Railway Safety Directive)

"'Type' of service is characterised by passenger transport, including and excluding high-speed services, freight transport, including and excluding dangerous goods services, and shunting services only.

'Extent' of service and of the railway undertaking is characterised by volume of passenger/goods and the estimated size of the railway undertaking in terms of employees working in the railway sector (micro, small, medium sized, large enterprise).

'Type' and 'extent' of services for all Part B Certificates, carried out globally by the same railway undertaking in one or more States, must be covered by 'type' and 'extent' of services of the Part A Certificate."

Guidelines for compilation, Regulation 653/2007/EC

5.1 General context

According to Article 10 and Article 11 of RSD, the national safety authority shall grant the safety certificate to the RU and the safety authorisation to the IM. The safety certificate/authorisation provides the evidence that the company has established its safety management system in conformity with the applicable European

and national legislation requirements and that the company is capable of controlling the risks associated with its activities and can thus operate safely its business.

According to RSD, the safety certificate/authorisation needs then to be updated when the RU/IM makes substantial changes to the type and extent of the operation. Those changes can be of technical, operational or organisational nature. Nevertheless, the RSD does not define nor provides guidance on what is meant by "substantial change".

An updated (or amended) safety certificate (or authorisation) shall be necessary in case of substantial changes occurring before the expiration of the safety certificate (or authorisation) in accordance with the provisions set out in Article 10(5) and Article 11(2) of RSD. A renewal of a safety certificate (or authorisation) is necessary for those RUs/IMs already granted with a safety certificate (or authorisation) that are willing to continue their railway operations after the expiration of their current safety certificate (or authorisation).

The sections below are a reminder of the provisions and tools in place for both the RU/IM and NSA to manage safely and monitor the effectiveness of changes to the railway system. The objective is to enable the NSA to determine consciously where its resources should be used at best and which activities should be given priority over unnecessary intensive administrative work.

5.1.1 Provisions in the SMS for a safe change management

In order to manage safely technical, operational or organisational changes to the railway system, as part of the SMS arrangements :

(a) the RUs and IMs must establish a change management process[14]. For that, CSM Regulation on risk evaluation and assessment 402/2013/EU is the cornerstone of the SMS that the RU/IM uses to determine whether the change is significant or not in terms of risk assessment:

(1) **if the change is significant**, the CSM Regulation on risk evaluation and assessment 402/2013/EU must be applied fully, including the process in Annex I for risk assessment and risk management. An accredited or recognised CSM assessment body must also be appointed in order to check the correct application of the above CSM Regulation and the appropriateness of the risk assessment results to fulfil safely the intended objectives of the change;

(2) **if the change is not significant** but nevertheless is safety relevant, the use of the risk management process in Annex I of the CSM Regulation on risk evaluation and assessment 402/2013/EU is not compulsory. However, the SMS must anyway have appropriate risk assessment and risk management processes in order to control the associated risks to an acceptable level.

As a result of application of these risk assessment and risk management processes of the SMS, the RU/IM is able to identify risk control measures necessary to keep the residual risks to an acceptable level.

(b) in compliance with the CSM Regulation on monitoring 1078/2012/EU, the RU/IM must also have a monitoring process in place that shall :

(1) monitor the effectiveness of all processes and procedures of the SMS, including the effectiveness of technical, operational and organisational risk control measures identified by the risk assessment and risk management processes described above;

[14] *This requirement results from point 2(d) in Annex III of Directive 2004/49/EC and from criterion M in Annex II of the Regulations (EU) N°1158/2010 and (EU) N°1169/2010 on the CSM for Conformity Assessment.*

(2) identify as early as possible instances of non-compliance with the expected objectives and that might result in accidents, incidents, near-misses or other dangerous occurrences;

(3) identify and implement appropriate preventive, corrective or both types of measures for the non-compliances that are considered unacceptable.

(4) for transparency reasons, the RU/IM shall document[15] the results of risk assessment, risk management, change management and monitoring processes.

These processes of the SMS enable the RU/IM to **Plan-Do-Check-Act/Adjust (PDCA)** safely changes related to its business through :

(a) the systematic identification of all reasonably foreseeable risks arising from changes;

(b) the definition and implementation of risk control measures to keep the risks acceptable;

(c) the monitoring of the correct implementation and of the effectiveness of those risk control measures;

(d) if risk control measures are found to be ineffective, the definition of an action plan with appropriate preventive, corrective or both types of measures in order to ensure a continuous achievement of safety performance of the railway system;

(e) the transparent documentation of results of risk management, change management and monitoring processes.

Therefore the provisions in the SMS allow the RU/IM to manage effectively and safely all its activities and operations. This is in line with the Safety Directive which requires those who create the risks to control them.

In order to comply fully with Article 10(5) and Article 11(2) of RSD, the RU/IM's SMS should also have in place a process for notifying to the NSA changes that might require the update of the safety certificate (or safety authorisation).

As part of the safety certification (or authorisation), the NSA assesses the RU/IM's ability to manage safely changes to its business, to monitor the effectiveness of the risk control measures identified by the risk management and, when necessary, to undertake automatically appropriate preventive, corrective or both types of measures in order to ensure a continuous achievement of safety performance of the railway system.

5.1.2 Supervision activities

According to Article 16(2)(e) of RSD and CSM Regulation for Conformity Assessment 1169/2010/EU and CSM Regulation for Conformity Assessment 1158/2010/EU, after the award of the safety certificate (or authorisation) the NSA shall supervise the RU/IM in order to :

(a) verify on the one hand that the processes and procedures of the SMS are actually applied by the RU/IM and, on the other hand that the SMS is fully functional and effective;

(b) verify that the RU/IM is monitoring the effectiveness of its SMS according to the CSM Regulation on monitoring 1078/2012/EU and, when necessary, that the RU/IM defines appropriate action plans with preventive, corrective or both types of measures for the identified non-compliances.

Knowing that the risk assessment, risk management, change management, monitoring and documentation management processes are also part of the RU/IM's SMS, during the supervision activities of the SMS, the NSA has the possibility to :

(a) check the safe management of technical, operational and organisational changes by the RU/IM;

[15] *This requirement results from point 2(g) in Annex III of Directive 2004/49/EC, Regulation (EU) N°402/2013 and Regulation (EU) N°1078/2012.*

(b) check the correct application and the associated results of the risk assessment and risk management processes for both significant and non-significant changes;

(c) check the documentary evidences resulting from the application of those processes and in general the compliance with the documentation management processes of the SMS;

(d) check, including for non-significant changes, the implementation and effectiveness of the identified risk control measures;

(e) check the effectiveness of the RU/IM monitoring activities for the risk control measures defined by the risk assessment and risk management processes and the actual correction of the identified non-compliances;

(f) cross-check the changes notified (or not notified) to the NSA with all the changes implemented by the RU/IM.

According to the CSM Regulation on supervision 1077/2012/EU:

(a) the supervision enables the NSA to identify the areas of non-compliance related to continued application of the SMS and to the safety regulatory framework;

(b) the NSA shall share the results of the supervision with the RU/IM on the effectiveness of their SMS in delivering safe performance and the areas of non-compliance. The RU/IM is required to propose action plan or plans for managing those non-compliances;

(c) the NSA shall evaluate the appropriateness and implementation of the RU/IM action plan or plans to remedy those non-compliances.

The supervision activities enable thus the NSA to have an overview of the safety performance of the RU/IM and to gain trust and assurance in the safe management and control of their activities and business through continuous application and improvement of the RU/IM SMS.

5.1.3 Assessment of the need to update a safety certificate or safety authorisation

From the previous sections, it can be summarised that:

(a) the RU/IM establishes and uses an SMS to ensure the control of all risks associated with its activities, including the safe management of changes. As part of the SMS, the RU/IM monitors also the correct application and the effectiveness of the SMS prescriptions and risk control measures identified by the risk assessments and risk management taking, where necessary, preventive or corrective actions to ensure a continuous achievement of the safety performance;

(b) the NSA is responsible for granting the safety certificate (and safety authorisation). After the award of the safety certificate (or authorisation), the NSA oversees the safety performance of the RU/IM, requesting them as appropriate to provide action plan(s) for correcting the identified non-compliances;

(c) the RSD sets out the conditions for the update of the safety certificate. The type and extent of railway operations are defined in the guidelines annexed to Regulation 653/2007/EC;

(d) Article 10(5) of RSD requires the holder of the safety certificate to **inform the NSA of all major changes** in the conditions of the relevant part of the safety certificate;

(e) Article 11(2) of RSD requires the holder of the safety authorisation to **inform the NSA of all substantial changes** made to the infrastructure, signalling or energy supply or to the principles of its operation and maintenance.

How can the NSA determine whether an update of the safety certificate (or authorisation) is needed?

(a) the question of new or increased risk for the railway company operations may need to be considered as a parameter, although in some cases, an update of the safety certificate (or authorisation) may be required when risks could be considered to be reduced by either :

(1) changing the type of operation to a potentially lower risk type such as for example changing from "freight transport including dangerous goods" to "freight transport without dangerous goods", or;

(2) substantially reducing the extent of their operation;

(b) considering the provisions in the RU/IM's SMS concerning the processes for "change management" and "notification of changes to the NSA" (see section 5.1.1), the RU/IM shall inform the NSA about the intended change and the process used for its safe management, including the production of relevant documentary evidence.

(c) based on this information and that collected by the NSA during the supervision of the RU/IM, the NSA should :

(1) evaluate whether the change and its inherent risk(s) are already adequately managed and controlled safely by the RU/IM through its SMS arrangements;

(2) decide whether reassessment of the SMS, and thus update of (part(s) of) the safety certificate (or authorisation), is needed at all. The assessment undertaken by the NSA to decide whether (or not) the safety certificate (or authorisation) is to be amended should be informed by the supervision of the RU/IM by the NSA;

(3) publish the criteria by which the NSA will decide when the update of the safety certificate (or authorisation) is likely to be required;

(4) evaluate the adequacy of the existing supervision strategy and plan and update it as appropriate with any additional supervisory tasks to control the correct and effective application of both the SMS processes and risk control measures identified by the RU/IM's risk assessment and risk management processes.

In case the update of the safety certificate (or authorisation) is necessary, the scope of the SMS reassessment should in any case be proportionate to the level of risk introduced by the change(s) and focus on the relevant areas.

5.2 Update of safety certificates

5.2.1 Legal requirements

The RU is the one responsible for requesting the update of the safety certificate if the *"type or extent of the operation is substantially altered"*.

The update of the safety certificate should not be on the initiative of the NSA but the result of an application from the RU. During its continuing supervision, the NSA may take enforcement actions as appropriate to ensure that the RU still meets the applicable requirements. This could lead to an update of the safety certificate (e.g. with conditions of use).

5.2.2 Definition of the "type" and "extent" of operation

The guidelines annexed to Regulation 653/2007/EC on the use of a common European format for safety certificates and application documents define the "type" and "extent" of operation as follows :

(a) *"« **Type** » of service is characterised by :*

(1) *passenger transport, including and excluding high-speed services;*

(2) *freight transport, including and excluding dangerous goods services, and;*

(3) *shunting services only*.

(b) *« **Extent** » of service and of the railway undertaking is characterised by :*

(1) *the volume of passenger/goods, and;*

(2) *the estimated size of the railway undertaking in terms of employees working in the railway sector (micro, small, medium sized, large enterprise)*.

(c) *« **Type** » and « **extent** » of services for all Part B Certificates, carried out globally by the same railway undertaking in one or more States, must be covered by 'type' and 'extent' of services of the Part A Certificate*."

5.2.3 Change of safety regulatory framework

Any "*substantial change in the safety regulatory framework*" (e.g. a new version of a relevant EU directive or regulation, a national regulation including new or revised notified national safety rules) has to be identified and managed by the RU through its SMS processes (compliance with legal and other safety requirements, change management process). The RU is then responsible to comply with the new requirements. As part of its duties, the NSA has to promote the safety regulatory framework. Therefore, the NSA should give support to the RU in understanding the content of the changes made to the safety regulatory framework.

Knowing that the SMS requires a procedure to ensure the compliance with new regulations and standards, the effectiveness of this procedure can be continuously controlled through the NSA supervision. In case of non-compliance, the NSA can take appropriate enforcement actions, e.g. conditions (or limitations) of use in the safety certificate or as a last resort solution, its revocation.

5.2.4 Notification of changes

The NSA should be informed of changes when there are "*major changes in the conditions of the relevant part of the safety certificate*" or when "*new categories of staff or new types of rolling stock are introduced*" (Cf. Article 10(5)(b) of RSD). That includes:

(a) the changes that do not conform to a SMS provision described in the application submitted to the NSA when applying for a safety certificate; or

(b) some aspects of the change that are not covered by what is described in that application because it introduces a novelty not covered by the SMS provisions.

Although a RU does not modify its core business, the way the business is organised or achieved might change. For example, training of staff, or maintenance activities of passenger vehicles might be done internally whereas they were previously subcontracted to external companies. Those changes create new interfaces and new responsibilities within the RU. In order to manage safely such changes, new categories of staff or new equipments (including types of vehicles) might be required and new SMS processes and procedures need to be designed to organise the safety of those activities within the RU.

Such changes affect the conditions under which the safety certificate was delivered. The NSA should then control how these changes were managed by the RU through its SMS, including their reporting to the NSA as appropriate (See also section 5.1.1).

The NSA can still evaluate the adequacy of its supervision strategy and plan and update it as appropriate to include any additional supervisory tasks necessary to verify the correct and safe management of the change, including their notification (See also section 5.1.2). The NSA can always take enforcement actions as appropriate to ensure that the RU still meets the applicable requirements.

The RU should notify relevant changes to the NSA and it should be discussed together whether or not it leads to an update of the safety certificate.

Based on the requirements in Article 10(5) of RSD, "**substantial changes**" made to the the "type or extent of the operation" should require the update of the safety certificate.

Considering the explanations in section 5.2.2, "substantial changes" relate to changes of core business of the RU, i.e. changes to "passenger transport", including/excluding high-speed services, to "freight transport", including/excluding dangerous goods services, and to "shunting only".

For example, the emergency management procedures depend on whether the freight transport includes or not dangerous goods. Such a change requires important changes to the SMS. The NSA might want to reassess the changes in order to verify that appropriate processes and procedures are put in place by the freight operator. Consequently, an update of the safety certificate might be necessary.

5.2.5 Examples of changes that could require the update of a safety certificate

If the SMS is updated and needs to be reassessed, the scope of the reassessment should be proportionate to the level of risk introduced by the changes.

The following three fields concern the "type and extent" of operation of the RU :

(a) type of service[16];

(b) volume of goods/passengers, and;

(c) number of employees (or size of the company).

These three fields provide the basis for the assessment of whether changes in "type and extent" of operation are substantial or not.

Any change of operation affecting these three fields needs an update of the safety certificate. This applies whether the change concerned arises from business developments within a company or from the taking over of another company operation.

For example, if a railway undertaking delivering passenger transport intends also to operate freight transport, either after merging with or acquiring another company, this should be considered as a "substantial change" in the "type and extent" of the service delivered by the railway undertaking. Both Part A and Part B safety certificates should then be updated.

If the change does not affect those three fields of the safety certificate, or if the need for update of the safety certificate is not obvious, the questions of new or increased risk for the railway company operation may need to be considered as a parameter and whether the change can be managed safely through the safety management system of the railway undertaking. As already mentioned, the scope of the SMS reassessment should in any case be proportionate to the level of risk introduced by the change(s) and to the nature and significance of the change(s) :

(a) Example 1: a change of legal denomination of the railway company requires the update of the certificate. However, the change of legal denomination of the railway company should not require the reassessment of the RU SMS. It is an administrative act;

(b) Example 2: changes to a lower risk (e.g. change from passenger transport including high-speed services to passenger transport excluding high-speed services) is generally an administrative exercise with only minimal checks on the implications for the railway company SMS;

(c) Example 3: changes to a higher risk (e.g. from freight transport excluding dangerous good services to freight transport including dangerous good services) should be regarded as a substantial change.

[16] *The main "types of service" are "passenger transport", including/excluding high-speed services, "freight transport", including/excluding dangerous goods services, and "shunting only".*

This should require the assessment of the changes to the SMS provisions and the update of the safety certificate;

(d) changes that potentially create higher risks for the operation could be regarded as substantial ones and might therefore require the assessment of the changes to the SMS provisions and possibly the update of the safety certificate :

(1) Example 4: introduction of "Driver Only Operation" within a company operating before the change with on board guard or staff assisting the driver at platform operations should be regarded as a substantial change;

(2) Example 5: freight operators which go into the passenger market either running charters or ancillary services[17] to passenger train operators should be regarded as a substantial change;

(e) Example 6: considering that the internal restructuring of a railway company could have adverse effects on its SMS arrangements and that the existing processes and procedures of the SMS need to be redesigned or new ones to be developed, such a change could be considered as a substantial change that requires a deeper and more complete reassessment of the RU SMS;

(f) Example 7: an RU starting new operation in another Member State, especially for cross-border traffic, may be identified as an operational change. This requires the application of the CSM for risk assessment [3] and, as a result of that, may also require changes in the SMS arrangements depending on the risk control measures identified by the RU. Such changes might thus require the RU SMS to be wholly or partly reassessed.

In general the provisions in the Part A[18] of the safety certificate should be laid down in such a way that they are valid for the infrastructures of different Member States.

The assessment of whether a change in the "**extent of services**" should be considered as a substantial one or not needs to be done on a **case-by-case basis**. Once again, the major parameter to consider is whether the change increases the risk(s) or introduces new risk(s) to the railway company operation and whether the change can be managed safely through the safety management system of the railway undertaking. The scope of an SMS reassessment should in all cases be proportionate to the level of risk introduced by the change(s) and to the nature and significance of the change(s) :

(a) Example 8: the change of route could be substantial if an operation is proposed for a line or a part of the network on which there was previously no operation by that railway undertaking (except for temporary diversions) and this new route would increase the risk (e.g. exposure to a new risk for that railway undertaking). An example of such a change can be the operation through a sub-surface station or lengthy tunnels;

(b) Example 9: an increase in the frequency of service could increase the risk for the railway undertaking, e.g. potential risks arising from congestion. Such changes should not be considered as substantial ones; they can be managed safely through the SMS of the railway undertaking. As described in section 5.1.1 :

(1) the SMS has processes and procedures in place to keep risks under control and to take appropriate preventive or corrective actions in case of detection of non-compliances during the monitoring of the operation by the railway undertaking;

[17] *The RU may have a diverse and flexible fleet delivering various type of services such as freight operations (main business) and passenger & train operating company support (to other RUs).*
[18] *The Part A safety certificate is valid throughout whole EU.*

(2) the railway undertaking notifies changes to the national safety authorities, so that the NSA is able to identify the additional supervisory tasks to be included in its strategy and plan for the supervision of the railway undertaking;

(c) Example 10: similarly, an increase in "route passenger-km per year" or "freight tonne-km per year" might increase the risk as the scale of the operation is affected. However, such changes and the associated risks can also be managed safely through the RU's SMS. The NSA can verify how this is done during the supervision activities of the railway undertaking into account the change management information notified by the RU.

5.3 Update of safety authorisations

5.3.1 Legal requirements

The IM is the one responsible for requesting the update of the safety authorisation if *"substantial changes are made to the infrastructure, signalling or energy supply or to the principles of its operation and maintenance*".

In all these cases, the update of the safety authorisation should not be an initiative of the NSA but the result of an application from the IM. During its continuing supervision, the NSA may take enforcement actions as appropriate to ensure that the IM still meets the applicable requirements. This could lead to an update of the safety authorisation (e.g. with conditions of use).

5.3.2 Change of safety regulatory framework

Any "*substantial change in the safety regulatory framework*" (e.g. a new version of a relevant EU directive or regulation, a national regulation including new or revised notified national safety rules) has to be identified and managed by the IM through its SMS processes (compliance with legal and other safety requirements, change management process). The IM is then responsible to comply with the new requirements. As part of its duties, the NSA has to promote the safety regulatory framework. Therefore, the NSA should give support to the IM in understanding the content of the changes made to the safety regulatory framework.

Knowing that the SMS requires a procedure to ensure the compliance with new regulations and standards, the effectiveness of this procedure can be continuously controlled through the NSA supervision. In case of non-compliance, the NSA can take appropriate enforcement actions, e.g. conditions (or limitations) of use in the safety authorisation or as a last resort solution, its revocation.

5.3.3 Notification of changes

The NSA should be informed of a change when *substantial changes are made to the infrastructure, signalling or energy supply or to the principles of its operation and maintenance* (Cf. Article 11(2)(a) of RSD). That includes:

(a) the changes that do not conform to a SMS provision described in the application submitted to the NSA when applying for a safety authorisation; or

(b) some aspects of the change that are not covered by what is described in that application because it introduces a novelty not covered by the SMS provisions.

As part of the SMS arrangements and in particular its change management process, the IM should be able to manage safely the change and also notify the NSA of all relevant changes (Cf. Article 11(2)(a) of RSD).

The NSA can still evaluate the adequacy of its supervision strategy and plan and update it as appropriate to include any additional supervisory tasks necessary to verify the correct and safe management of the changes, including their notification (See also section 5.1.2). The NSA can always take enforcement actions as appropriate to ensure that the IM still meets the applicable requirements.

The IM should notify relevant changes to the NSA and it should be discussed together whether or not it leads to an update of the safety authorisation.

Based on the requirements in Article 11(2) of RSD, "**substantial changes**" made to the "infrastructure, signalling or energy supply or to the principles of its operation and maintenance" should require the update of the safety authorisation.

5.3.4 Examples of changes that could require the update of a safety authorisation

As stated in Article 11(2) of RSD, the safety authorisation should be updated in case of substantial changes to :

(a) infrastructure, including control-command and signalling subsystems;

(b) any energy supply used in connection with the infrastructure, or;

(c) the principles of operation and maintenance of the infrastructure or energy supply.

The assessment of whether a change in any of the above categories should be considered as substantial needs to be done on a case-by-case basis. In practice, the major parameter to consider is whether the change increases the risk(s) or introduces new risk(s) to the infrastructure manager and whether that change can be managed safely through the safety management system of the infrastructure manager. In addition to that, the scope of an SMS reassessment should in any case be proportionate to the level of risk introduced by the change(s) and to the nature and significance of the change(s).

Substantial changes to the **infrastructure** could include :

(a) any completely new line that uses novel technology, e.g. fundamentally new forms of track-bed construction or new tunnels, bridges, viaducts that involve new technology in their construction specific risks;

(b) any major structure of a type that did not previously exist on the infrastructure, e.g. tunnels, viaducts, level crossings, new stations such as sub-surface stations that introduce specific risks;

(c) new types of signalling systems;

(d) new connections to other infrastructures which could give rise to a considerable increase in local traffic flow on the infrastructure in question and, as a result, an increase in risk.

Substantial **changes of energy supply** could include :

(a) introduction of an energy supply that currently does not exist and which requires its own permanent infrastructure, e.g. electrification of a line;

(b) introduction of an energy supply which requires its own permanent infrastructure and significantly different to the existing one, e.g. change from 3rd/4th rail to overhead supply, or;

(c) other changes to the energy supply which modify the level of the existing risks or create new risks, e.g. when the source of energy is not solely contained within the vehicle itself.

Change in principles of operation and maintenance :

(a) substantial changes in the principles of operation could include :

  (1) introduction of fully automated working to safety critical areas, or;

  (2) introduction of novel signalling systems e.g. the European Rail Transport Management System;

(b) substantial changes in the principles of maintenance could include :

  (1) significant changes in maintenance intervals for safety critical infrastructures;

(2) changes to automated maintenance systems, or;

(3) management of infrastructure maintenance by a contractor, or;

(4) management of the infrastructure maintenance within the company whereas previously this was done internally within the infrastructure manager.

From the above examples, decision on whether a change is substantial should also be thought about in the sense of (change of) scale. Indeed, changing one item of equipment could not be a substantial change. For example, changing one or two level crossings to a new type could not be a substantial change but changing multiple level crossings to a new type could be.

6 Safety assessment process

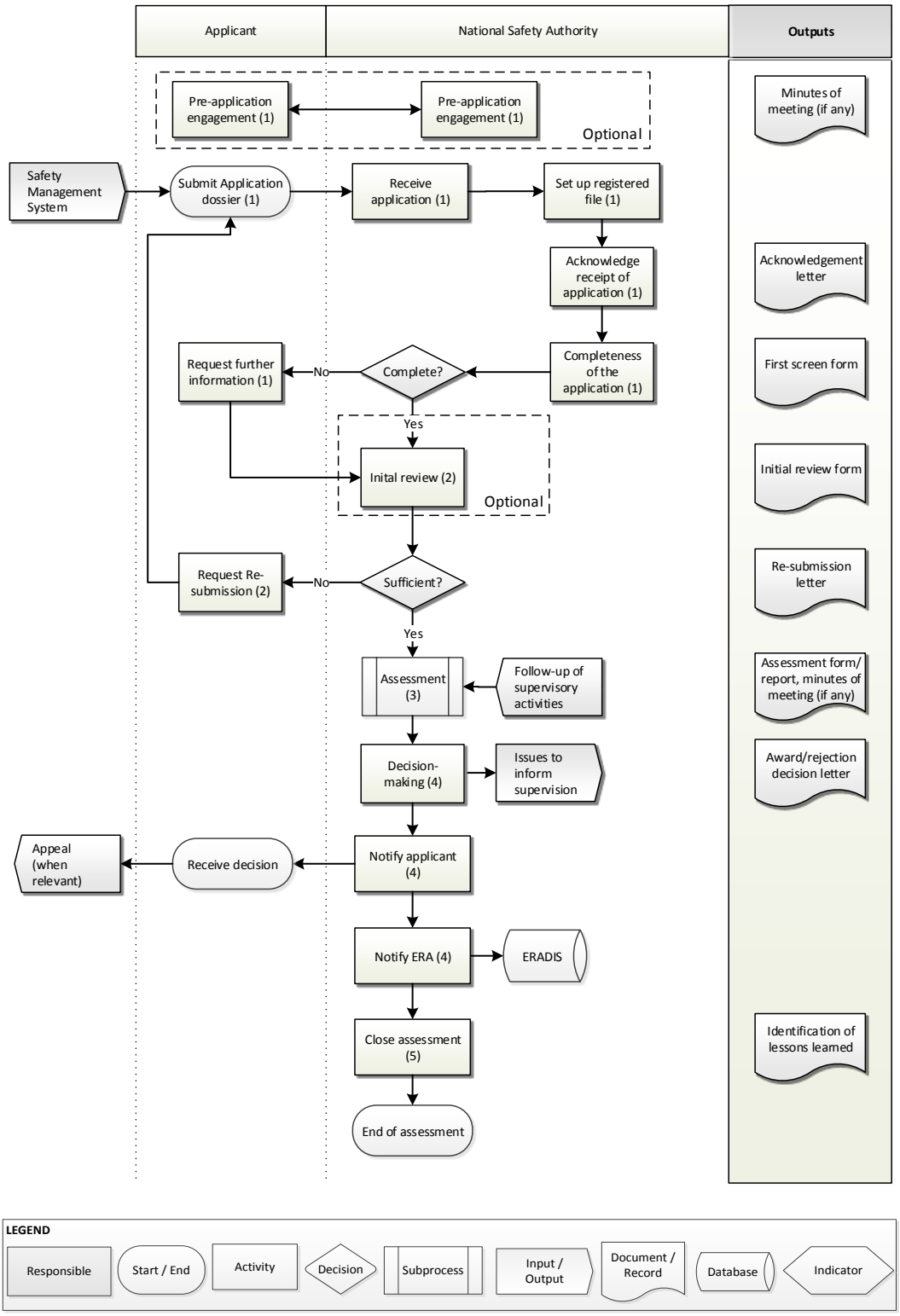


Figure 1: Safety assessment process.

6.1 Pre-application engagement and receipt of application

Pre-application engagement between the applicant for a safety certificate (or authorisation) and the NSA may be established upon request from the NSA or the applicant before submitting the application for a safety certificate (or authorisation).
This can help to:

- Facilitate early contact;
- Develop the relationship between assessor and applicant;
- Gain familiarity with applicant's safety management system; and
- Verify that the applicant has been provided with sufficient information so that it knows what is expected from it and the way the assessment process will be conducted and how decisions will be made.

It is usually good practice to convene a pre-meeting between interested parties to discuss the application in general terms. The pre-engagement should not be a means for the applicant to abuse the system, e.g. by escaping fees and charges and/or using the NSA as a free consultancy, so as to avoid the rejection of the application.

The NSA is however required to describe and explain the requirements for the safety certificates and list the documents that must be submitted in an application guide and make it available to the applicants free of charge (Cf. Art. 12(3) of RSD). Though similar provision does not exist for safety authorisation, the NSA is encouraged to include the same level of information for Infrastructure Manager(s) in its application guide. The NSA may also request the applicant to point out where in its application file the assessment criteria of the relevant CSM for Conformity Assessment [4][5] are met.

After receiving the application dossier, the NSA sets up the registered file and formally acknowledges receipt of the application (e.g. by letter). The date of acknowledgement of receipt being the start date of the safety assessment process against which the process duration can be monitored. The NSA has established that the necessary resource is available for this assessment to be timely completed (i.e. no longer than four months provided that all information required and any supplementary information requested by the NSA has been submitted).

Document control is exercised through the registered file[19] which should contain all papers relating to the receipt, handling, assessment and assurance of the application and the final decision over issue of a safety certificate (or authorisation) and a copy of the safety certificate (or authorisation).

The NSA undertakes a first screen of the application to check that all the documentation is complete. The first screen is essentially an administrative task and can be carried out by local administrative staff so long as they have sufficient familiarity with safety certificate (or authorisation) applications. The results of this should be recorded, e.g. using the 'first screen' form (See Annex 6.1).

The objective is to establish if the applicant has provided the basic information which is either required by the EU Regulations or needed for it to be processed effectively. The application shall comply with and at least include the documents identified in Annex III of Regulation 653/2007/EC. Though not prescribed by EU Regulation, standard application form and format for safety authorisation are recommended for use (See section 3.2).

The application can be for:

- a first safety certificate (or authorisation);

[19] *By definition, a file means "a collection of information about a particular person or thing" (Oxford Dictionary). It does not necessarily refer to an electronic file.*

- an amended (or updated) safety certificate (or authorisation), in case of substantial changes occurring before the expiration of the safety certificate (or authorisation) in accordance with the provisions set out in Article 10(5) and Article 11(2) of RSD (See also section 5); or
- a renewal of safety certificate (or authorisation), prior to the expiration of the safety certificate (or authorisation).

Where the application is for both a safety certificate and a safety authorisation (i.e. the case of a vertically integrated operation), the NSA should also check that the different parts of the application are clearly distinguishable, and, in the case of those parts which are relevant to both, indicate clearly that this is so. In addition, Member States may have exclusions (or not) from the obligations of having a safety certificate (or authorisation) (Cf. Article 2 of RSD). Depending on what is not excluded from the scope of application of RSD (e.g. regional network), the NSA should check that the evidence for such operation is clearly identified.

For a renewal, the NSA should check details of changes to the evidence previously submitted for the first safety certificate (or authorisation). The renewal application is therefore expected to describe changes to information previously sent to the NSA for the first application and to give an indication of where the evidence against each criterion can be found in the SMS. In addition, the NSA should take note of its continuous supervisory activity to identify issues to be scrutinised during re-assessment. Based on both the changes made to the SMS since the first application and the results of its supervisory activities, the NSA identifies the relevant criteria set out in the CSM upon which to assess the renewal application. The NSA must have a targeted and proportionate approach to re-assessment. Using the results of its supervision to inform re-assessment enables the NSA to reach this objective. Therefore, the full re-assessment of the SMS on each renewal application is not necessary.

Having an authorisation for placing into service new rolling stock shall not be a pre-condition for applying for a safety certificate; this is to allow on-track tests of new rolling stock before authorisation for placing in service has been given by the NSA. However, it does not prevent the Member States defining any operational and organisational arrangements for carrying out these tests (Cf. Art. 88 of Commission Recommendation (EU) No 2014/897 [8]).

If any of the required information is not provided or not clearly identified, then the applicant should be asked for the missing details as soon as the first screen of the application has been carried out, informing them that assessment cannot properly begin until it has been received. The request shall also include details of timescales for the applicant's response, proportionate to the difficulty of providing the information requested, and be recorded in the registered file. However if the applicant delays significantly providing this information, they should be informed that it may delay the final decision overall and, therefore, their ability to run operations from any specific date.

For applications made with an existing Part A, the NSA will at this stage need to make a judgment on whether the operation for which the Part B application is made is equivalent. This judgment should be based on the broad risk profile with respect to the type and extent of the operation for the existing Part A and the proposed Part B. If the NSA comes to the view that the operations are not equivalent, it should then notify the applicant that they need to update their existing Part A safety certificate (See also section 5) and submit a new Part A application to accompany the Part B application. For example, if the Part A safety certificate does not cover the transport of dangerous goods, a Part B safety certificate cannot be granted to the RU for this type of service.

For a safety certificate, amendments (or updates) are required when there is a substantial change proposed to the type and extent of an operation (Cf. Art. 10 of RSD), and for a safety authorisation when there is a substantial change proposed to the infrastructure, any energy supply used in connection with the infrastructure or the principles of operation and maintenance of such infrastructure or energy supply (Cf. Art. 11 of RSD). Additional information can be found in section 5 of this document. It is likely that the NSA will receive information from the applicant alerting it to the possibility of an amendment prior to an application being made, or the applicant may ask the NSA's opinion on a whether proposed change merits an

amendment or just notification. If neither has happened, the NSA should check firstly that the change for which the application is made is clearly described and, secondly, that it is genuinely for a substantial change (See also section 5). The NSA may need to make further enquiries with the applicant before coming to a conclusion, but if the NSA considers the proposed change not to be substantial it should inform the applicant in writing that an amendment is not required, keeping a record of the decision for the registered file.

For Railway Undertakings, an application for an amendment (or update) of the safety certificate can be made for either a Part A or Part B alone or for both simultaneously. Where the application is for an amendment to a Part B certificate only, the NSA should check that it would still be equivalent, if the changes were made, to the type and extent of operation for which the Part A is valid. If this is considered not to be the case, the NSA should notify the applicant that its application has been refused and that an application for a new (Part A and B) certificate should be made instead.

There should be a maximum of four months from the start of the assessment for processing an application if the information submitted and any reasonable supplementary information requested by the NSA has been supplied. The assessment period could be shorter; for example, where the scale of changes since the previous application is small. In any case, the NSA should check there is sufficient time for:

- First applications, where an operation is planned to start on a particular date;
- Further applications (renewal), before the current safety certificate (or authorisation) expires;
- Applications for an amendment (or update), where a change is required to be implemented by a desired date[20].

For that purpose, the NSA may also find it helpful to retrieve from the European Railway Agency Public Database of Safety Documents (ERADIS) a list and/or records of all valid certificates with expiry dates.

If the time is significantly shorter then contingency procedures may need to be invoked, which include notifying the applicant that there may be insufficient time (See also section 4). The applicant is however responsible for submitting its application within the appropriate timeframe as set out in the NSA's application guide to allow the NSA to carry out its assessment in normal conditions (i.e. prior to the expiry of the safety certificate (or authorisation).

All applications originating from railway companies based in other EU Member States must be in the language(s) permitted by the NSA's application guide. The NSA should 'sample' the application to check that the language is understandable. If it is clearly not, the NSA should discuss internally whether it should be returned, with a request for an improved version.

6.2 Initial review

The NSA conducts an initial review of the application by competent staff to make an initial judgement on the quality, sufficiency and appropriateness of the SMS and decides in which areas further information is necessary. The NSA may, as part of this request for more information, seek as much detailed information as it deems reasonably necessary to help its assessment of the application (Cf. Annex I point 3 of CSM for Conformity Assessment [4] or Annex I point 2 of CSM for Conformity Assessment [5]).

The objective is to establish if the application contains sufficient evidence and is presented clearly enough so that it can be properly assessed against the assessment criteria. It is not to identify shortcomings of a detailed nature but to determine whether there are deficiencies in the content of the application serious enough for it not to be worth spending further time on.

[20] *In some cases, national regulation may require that any change made under the terms of an amended (or updated) safety certificate (or authorisation) should not take place until it has been issued.*

This comprises a scan of the actual content of the evidence contained in the application (i.e. the summary of the manual of the SMS). The results of this should be recorded, e.g. using the 'initial review' form (See Annex 6.2 or Annex 6.3).

In some circumstances, such as where the NSA has already been consulted on the content of the application prior to formal submission (i.e. pre-application engagement), **the NSA may already know that it contains adequate evidence, in which case it will be possible to leave out this stage and move straight to the main assessment**. If this occurs, a note should be made for the file (See Annex 6.2 or Annex 6.3) so that there will be traceability of what has happened. It may also be that the results from any supervision activity provide sufficient knowledge of the applicant so a decision on the application can be made.

To conduct the initial review, the NSA should read the whole application, but should not assess against the criteria (i.e. check that evidence is provided against each of the criteria without getting assurance that it is sound evidence). For example, the 'initial review' form (See Annex 6.2 or Annex 6.3) has a column for comments to allow for observations which may aid the later detailed assessment. The principal considerations are:

- Determining whether the application is structured and internally cross-referenced (e.g. summary of the SMS with signposts to other procedures and rules) so as to permit assessment to be effective and properly recorded, i.e. adequate page/section/paragraph numbering, where appropriate different parts of the application clearly identifiable throughout and reflect what is indicated in the contents page (e.g. part A/part B, certificate/authorisation).
- Identifying whether evidence is provided against all relevant criteria.

The criteria which apply will differ according to whether it is a first, renewal or amendment (or update) of application. For a first application, all assessment criteria of the relevant CSM for Conformity Assessment [4][5] will apply. For renewal and amendment (or update) of applications, the applicable criteria may vary from one case to another, and while the NSA may make an initial judgement as to whether evidence for the correct criteria has been provided, this may not be fully evident until the detailed assessment is under way.

If the application is fundamentally deficient, such that it clearly could not lead to the issue of a safety certificate (or authorisation) without major revision, the NSA should discuss this internally without delay and if the conclusion is confirmed, the application should be returned immediately, stating the reasons in writing, asking the applicant to re-submit. The request shall also include details of timescales for applicant's response. The decision, the reasons for it and the timescales for response should be recorded in the registered file.

It should be noted that if the applicant fails this test, this may not amount to a formal refusal of the application but could instead be a request for 'further information'. However this is one set of circumstances where the period for assessment would probably have to be protracted.

If this jeopardises the ability of the applicant to obtain a safety certificate or authorisation before the expiry of an existing one, then contingency procedures may need to be invoked, which include notifying the applicant that there may be insufficient time.

Where it is felt that the quality of the application is lacking but not to the extent that a re-submission is required, for example information is missing against one or two criteria, while the rest seems sound, the NSA should request the relevant further information at this stage and should not wait until the main assessment is complete.

The initial review may show that the application contains superfluous information. The application should be concise and self-contained with all relevant information provided within it. Other documents should only be referenced, so that, firstly, NSA's assessor(s) can have confidence that they exist, and secondly, so that they can be requested for examination after the issue of the safety certificate (or authorisation) during subsequent supervision (e.g. audit, inspection). An application may reproduce extracts from the relevant documents

within the body of its text, but in general the assessor should not have to refer to other documents to obtain the required evidence.

Any supplementary documents sent as part of the application and/or information in appendices should be kept on file and where relevant, shared with whom it may concern within the NSA.

Even where an application is self-contained, it may be excessively long and detailed. An application is sufficient when it meets the assessment criteria of the relevant CSM for Conformity Assessment [4][5].

6.3 Assessment

The NSA should proceed to the detailed assessment (See Figure 2) after the initial review, using the assessment criteria of the relevant CSM for Conformity Assessment [4][5]. In undertaking this, the assessors will be exercising professional judgment and should provide and document reasons for conclusions reached (See Annex 6.4).

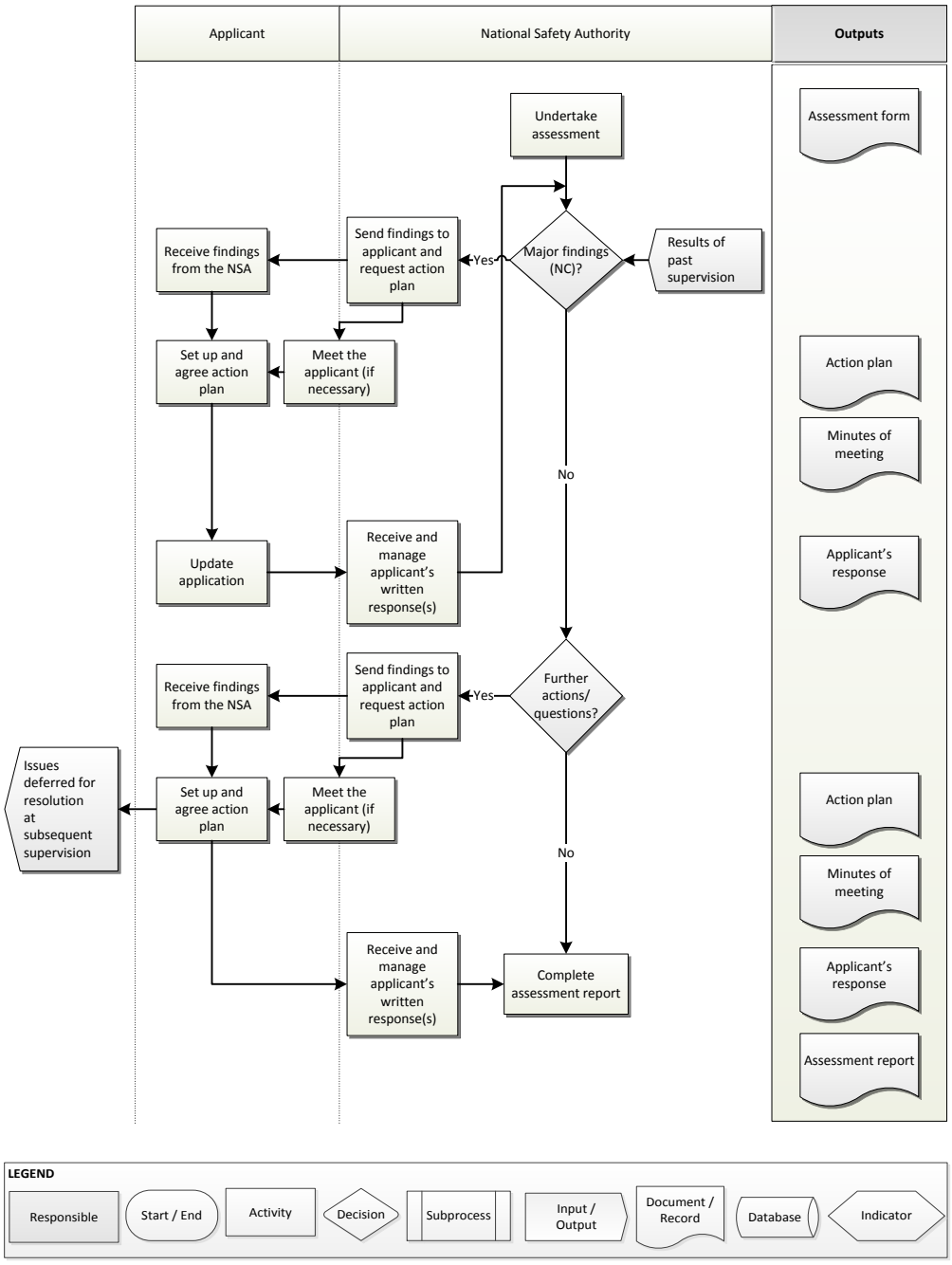


Figure 2: Detailed assessment process.

The deadline for the completion of the assessment should be confirmed by the accountable manager[21] to the assessor(s). The NSA shall have arrangements in place to ensure that the assessor(s) complete agreed tasks to time.

The assessor(s) should determine:

› Whether the assessment criteria are complied with;

[21] *The same person within the organisation may assume different roles. For example, the person carrying out the role of accountable manager can be a peer at the same functional level (i.e. an assessor appointed to another application dossier), under the condition that s/he is given the authority to act and that s/he is independent of the assessor(s) in charge.*

- Where there is non-compliance, whether further information should be requested or the matter can be deferred to supervision after issue of the safety certificate (or authorisation); and
- Whether there are any other points for later supervision.

The NSA shall give reasons for issuing a safety certificate (or authorisation) and these fundamentally hinge on compliance with the relevant CSM for Conformity Assessment [4][5] and consequently the assessment criteria. For this reason, those criteria which have been complied with should be listed on the assessor's report as well as those where compliance is not complete or fully apparent. This will inform a balanced decision on whether to issue a safety certificate (or authorisation).

Where any non-compliance is identified, this will not necessarily mean that the application will be rejected. There will be different degrees of non-compliance or deficiency (i.e. major or minor):

- If it is a matter of substance (e.g. there is a concern about the ability of the applicant to operate safely), it is a major concern that will need resolution before the application can be accepted.
- If it is a minor concern only, it should be recorded and can be deferred for resolution at subsequent supervision (e.g. inspection).

The results of past supervision should help determine whether there are open non-compliances (or deficiencies) that need follow-up and inform the NSA's decision. For example, a safety certificate (or authorisation) could not be renewed if major non-compliance (or deficiency) within or with the SMS of the applicant is identified during supervision since the application must depend on the SMS meeting the assessment criteria.

The NSA should be transparent on how it judges non-compliances (or deficiencies) to be major or minor. It should also provide the applicant with a timescale for implementation of the agreed measures (action plan) based on the applicant's response(s).

When identifying a point of non-compliance, the assessor should be as specific as possible, to assist the applicant in understanding the level of detail expected in the response. To do this the assessor(s) should:

- Refer accurately to the relevant part of the application;
- Identify the relevant assessment criterion (Cf. Annex II of the relevant CSM for Conformity Assessment [4][5]), including any related regulations, rules, and standards;
- State why the assessment criterion is not met (e.g. due to lack of information or clarity); and
- Agree on further commitments, information and any supporting evidence to be provided, as required by the level of detail of the criterion and specify, in case of major deficiencies, after discussion and upon agreement of both parties, the timeframe for compliance[22].

The assessor(s) should document the assessment results (See Annex 6.4, Part 1).

The assessor should not demand more detail than what is required to have sufficient assurance that the criterion is met. Editorial or presentational concerns, or typographical errors, should not be taken as evidence that applicant has not demonstrated compliance unless they affect the clarity of the evidence provided by the applicant.

After completing the assessment, the NSA should inform the applicant of any issues of non-compliance and/or need for further information, e.g. by sending them a copy of the 'part one' of the assessment form (See Annex 6.4).

[22] *The applicant is responsible for proposing an action plan to rectify the deficiency in accordance with the agreed timeframe. In case of minor deficiencies not preventing the delivery of the safety certificate (or authorisation), both the NSA and the applicant may agree on a timeframe for compliance that can be extended beyond the start date of the new safety certificate (or authorisation). The completion and effectiveness of these actions can then be verified during subsequent supervision (e.g. audit).*

If there are significant matters to be raised, it is strongly recommended that the NSA meets the applicant as this is likely to be the quickest and most efficient way to resolve them. The NSA should confirm any pre-arranged date for this with the applicant or, otherwise arrange a date. In either case confirmation in writing (letter or e-mail) should be sent and acknowledgement requested. This confirmation can generally be sent with details of the issues to be raised.

The objectives of such a meeting are to:

- Ensure that the applicant has understood clearly the identified areas of non-compliance;
- Discuss what is required to remedy them;
- Agree the nature of the further information and any supporting evidence to be provided (action plan);
- Inform the applicant about issues that will be inspected early on during the supervision phase.

By this process, it is intended to avoid multiple exchanges of correspondence to resolve outstanding matters. Where there are several assessors involved, it may be useful for them to attend, so that they may represent their own findings accurately, particularly where specialist expertise is involved. Where it is intended to explore an interface issue, the NSA may also wish to invite other relevant parties to the meeting.

When arranging a meeting, the NSA is advised to obtain in advance details of who will represent the applicant. Minutes should be taken, with copies sent to all participants and placed on the registered file. Whatever the outcome, a formal written response from the applicant will always be needed to close matters out.

Whether there is a meeting or not, the applicant should send written responses (e-mail or letter) to all matters raised. The NSA should agree a timescale with the applicant for providing this response, informing them if this is not met, that the NSA might need to extend the time in which it reaches a final decision which could have implications for the operation either starting at a specified date, or continuing after expiry of the existing safety certificate (or authorisation), if the application is for a renewal.

All written and copies of electronic communications relating to the above should be placed in the registered file.

The applicant's written response(s) should be recorded for traceability purposes (See Annex 6.4, Part 1, column 'applicant's response'). When working with several assessors, it is recommended to provide the applicant with a single contact point, acting as liaison between the applicant and the assessors, for the collection and exchange of relevant information.

To be satisfactory, the applicant's written responses must be sufficient to allay the concerns expressed and to show that its proposed arrangements will meet the requirements of the relevant criteria within the CSM for Conformity Assessment [4][5]. It must include new text and/or rephrasing to replace what was unsatisfactory in the original application, with an explanation of how this deals with the identified deficiencies. The applicant may in addition supply relevant supporting SMS procedures as well as amending/adding relevant text contained in the original application.

Where a response is largely satisfactory, but there is a residual concern, it will be a matter of the assessor's judgment on how to deal with it. It may be appropriate either to raise this residual concern with the applicant or to defer complete resolution to supervision (See Annex 6.4, Part 2) after issue of the safety certificate (or authorisation). Whichever route is taken, the assessor(s) should record the decision with reasons. They should be able to objectively justify all findings and judgments which are recorded, in order to facilitate both the assurance process and the final decision, as well as to assist with any appeals against the final decision.

Where a response is considered unsatisfactory, it must be explained precisely why, identifying the further information or demonstration required of the applicant to make it satisfactory. Where there are significant inadequacies in the responses, the NSA should raise this as soon as possible with the applicant, if necessary arranging to meet them again or undertaking an inspection/audit of the relevant part(s) of its operation. It is

unlikely that a major re-submission of all responses would be required, but if this should be the case, the NSA should request this in writing.

The (lead) assessor should record any comments on the overall quality of the application (See Annex 6.4, Part 3).

If for whatever reason, a final resolution of any issue looks like becoming protracted such that the time limit may be exceeded, and deferment of concerns to a later supervision plan is not appropriate, the NSA should promptly discuss it internally. If concerns emerge that the application could be refused, or that it will take a longer time to reach a final decision than the period foreseen[23], the NSA would need to consider possible contingency procedures.

When the assessor(s) conclude(s) that either the application meets all requirements or that no further progress is likely with securing satisfactory responses to outstanding matters, s/he should complete the final assessment report (See Annex 6.5) which:

- States whether all criteria have been complied with or whether there are still matters outstanding;
- If the recommendation is to accept the application, compile items identified for inclusion in the supervision plan, including matters of residual concern not fully resolved during the assessment;
- Confirms that the application has been properly assessed;
- Gives the recommendation on whether to accept or refuse the application with a summary of the reasons, including an overview of the relative merits of the application; and
- Provides details of the appeal process with contact details.

The assessment report should also include:

- (where relevant) Any differences of opinion amongst assessors which required formal reconciliation (See Table 2, Part A in Annex 6.5);
- The follow-up of past supervision results (e.g. audits, inspections), accident/incident reports from railway companies, results of their internal audits and implementation of recommendations set out in the National Investigation Body's investigation report(s) to check whether all open points are closed since last assessment (See Table 3, Part A in Annex 6.5). These issues are acted on by the applicant during supervision and are finally closed-out (or not) in the assessment report.

It is also good practice to outline for traceability purposes:

- The purpose and scope of the assessment;
- The history of the assessment process until the final decision.

When completed, the assessor(s) signs and submits it to the accountable manager (e.g. line manager) along with the registered file.

The accountable manager should review the final assessment report and the associated assessment record, checking that the judgments and decisions made are documented, fair and consistent. There should normally be a discussion between the (lead) assessor and the accountable manager about this. If satisfied, the accountable manager should complete and sign his/her recommendations (See Part B in Annex 6.5) and return it to the file. If not satisfied, the accountable manager should review the issue(s) with the (lead) assessor and if agreement cannot be achieved, these (this) issue(s) should be resolved within the organisation at the appropriate level.

An assurance process should take place to ensure that the assessment process the process has been correctly applied. It is not intended to be a re-assessment of the application. The accountable manager or any other

[23] *Either in NSA's internal procedure and/or by national regulation.*

personnel independent of the assessor(s) within the organisation[24] should review the different records (i.e. forms and minutes of meeting if any), checking that:

- The different steps of the process have been correctly applied;
- There is sufficient evidence to show that all relevant aspects of the application have been assessed by at least one assessor;
- Written responses to all matters of non-compliance and requests for further information have been received from the applicant
- Issues of non-compliance were all resolved[25] or, where not resolved, the reasons for this were clearly documented;
- The recommendations given on the final assessment report reflect the assessment as a whole.

S/he should document her/his conclusion in the final assessment report (See Part C in Annex 6.5). If the conclusion is that the process has been properly followed it will be sufficient to confirm that the above steps have been followed accompanied by any qualifying comments. If the conclusion is that it has not, then reasons for reaching this should be clear and specific. The final assessment report should then be replaced in the registered file.

6.4 Decision-making

Based on the conclusions of the completed assessment, a decision must be made on whether to issue a safety certificate (or authorisation) or to refuse the application. Where a safety certificate (or authorisation) is to be issued it may identify some issues for later consideration in the supervision phase.

Once the decision has been taken and if the decision is to award the safety certificate or safety authorisation, the NSA prepares a safety certificate (or authorisation) for signing and stamping. Part A and Part B safety certificates shall use the standard format set out in Annex VI to Regulation 445/2011/EU (replacing Annex I of Regulation 653/2007/EC) and in Annex II to Regulation 653/2007/EC respectively. Safety authorisations may also use the standard format set out in Annex 2.

The NSA may decide to limit the scope of application of the safety certificate (or authorisation) if it finds that the applicant no longer satisfies the requirements on the basis of which it issued the safety certificate (or authorisation). The NSA may also decide to limit the duration of the safety certificate (or authorisation) if they conclude that there are good reasons to do so. If there is an action plan agreed with the applicant that the NSA can survey during its supervision, the decision to include limitations (or conditions) of use in the safety certificate (or authorisation) should only be the result of an enforcement action taken by the NSA to ultimately ensure compliance with the requirements of the relevant CSM for Conformity Assessment [4][5]. The NSA can always adapt its supervision plan to get assurance that the applicant can adequately manage the risks posed by its operations. For example, if the applicant is a new entrant that cannot immediately demonstrate the effectiveness of its SMS arrangements due to an insufficient number of railway operations during the period preceding the application, then the NSA can still decide to adapt its supervision plan to increase the frequency of audits/inspections. In this situation the NSA may decide to set specific audit objectives as appropriate in order to keep the applicant's activities under control (i.e. verification that it effectively does what it said it would do in its SMS).

Following this, the applicant will need to be informed about the final decision and a safety certificate (or authorisation) issued as appropriate.

If the decision is for refusal, the NSA should inform the applicant, giving the reasons for the decision (e.g. conditions of the certificate or the authorisation are no longer being met and significant risk arises as a result)

[24] *The same person within the organisation may assume different roles.*
[25] *Initial response deemed satisfactory; further exchanges undertaken with the applicant which resolved outstanding matters; or residual concerns deferred to later supervision.*

and notify them of the appeal procedure. As any refusal will have serious consequences, the NSA must ensure that before reaching any decision to refuse, all due process has been followed.

Irrespective of the decision, for greater transparency, it is advised that the assessment report is attached to or enclosed with the final decision.

The NSA shall notify the European Railway Agency within one month of each individual decision to issue, renew, amend or revoke safety certificates (Cf. Art. 10(6) of RSD) by means of ERADIS database (Cf. Art. 11(2) of Regulation (EC) 881/2004). It shall state the name and address of the Railway Undertaking (or the Infrastructure Manager), the issue date, scope and validity of the safety certificate (or authorisation) and, in the case of revocation, the reasons for its decision (Cf. Art. 10(6) and 11(3) of RSD). For Railway Undertakings, the NSA should also inform neighbouring and other NSAs where the Railway Undertakings (will) operate (if already known) (See ERA guidance on common approach to supervision of railway undertakings operating in more than one Member State [9]).

The NSA shall set out an appeal procedure for applicants to appeal against its decision and communicate it to the applicant.

6.5 Closing assessment

The NSA completes the administrative closure by ensuring that all documentation and records are reviewed, organised and archived. To continually improve its process, the NSA may decide to identify historic and lessons learned information for use by future assessments, leading possibly to the update of its organisational processes. This can include information on issues and risks as well as techniques that worked well that can be applied to future assessments and possibly shared with (or even learned from) other NSAs for continual improvement.

6.6 Assessment check-list

The following table can be used by the NSA to check the timely completion of the different tasks of the safety assessment process.

Table 1 : Assessment check-list

Name of applicant:		*Date application received:*
Task	*Target date*	*Completion date*
1. Notify assessor(s) of receipt of application	Immediate	
2. Set up the registered file	Immediate	
3. Acknowledge application		
4. First screen (Complete first screen form)		
5. Initial review (Complete initial review form)		
6. Initial review: if major deficiencies, inform applicant		Further information/fresh application received on:
7. Distribute application to assessor(s) (where relevant)		
8. Complete assessment (Complete assessment form)		
9. Meet applicant (where relevant)		
10. Send minutes of meeting to the applicant (where relevant)		
11. Receive applicant's response(s)		
12. Complete final assessment report (incl. assurance process)		The accountable manager signs the final assessment report: The assuror signs the final assessment report:
13. Prepare SC/SA		
14. Final decision/signature by delegated authority		
15. Notify applicant of decision (send SC/SA with reasons of decision)	Within 4 months of receipt of application (if no further information required)	

Table 1 : Assessment check-list

Name of applicant:		*Date application received:*
Task	*Target date*	*Completion date*
16. ERA notified (by ERADIS for safety certificate or by email for safety authorisation)	Within 1 month of decision/ signature	
17. Administrative closure (archiving/storage of the registered file)		

6.7 Records

The following table lists the records to be managed in a registered file by the NSA throughout the safety assessment process. The NSA may need a documented procedure to define the controls needed for the identification, storage, protection, retrieval, retention and disposal of records. The records may serve as inputs for management review and subsequent decisions to ensure the continuing suitability, adequacy and effectiveness of its processes.

Table 2 : List of records

Record name	*Storage responsible*	*Storage location*	*Minimum retention time*
First screen form			
Initial review form			
Assessment form			
Assessment report			
Acknowledgement letter			
Re-submission letter			
Decision letter			
Lessons learned/historical information			
Minutes of meeting			
Applicant's written response(s)			
Applicant's action plan			
Applicant's application dossier			

Annex 1 Standard application form for safety authorisation[26]

SAFETY AUTHORISATION APPLICATION

Application for Safety Authorisation confirming acceptance of the infrastructure manager's Safety Management System and the provisions adopted by the infrastructure manager to meet requirements necessary for the safe design, maintenance and operation in conformity with Directive 2004/49/EC and applicable national legislation

SAFETY AUTHORTY REFERENCE NUMBER

SAFETY ORGANISATION/AUTHORITY CONTACT INFORMATION

1.1. Safety organisation/authority addressed for the request

1.2. Complete postal address (street, postal code, city, country)

APPLICANT'S INFORMATION

2.1. Legal denomination

2.2. Infrastructure manager name

2.3. Acronym

2.4. Complete postal address (street,

postal code, city, country)

2.5. Phone number

2.6. Fax number

2.7. Email address

2.8. Website

2.9. National registration number

2.10. VAT No

2.11. Other information

Contact person information

3.1. Family name and first name

3.2. Complete postal address (street, postal code, city, country)

3.3. Phone number

3.4. Fax number

3.5. Email address

[26] *This application form is not prescribed by EU legislation but recommended for use.*

APPLICATION DETAILS

This application is for a

4.1. new authorisation ☐ 4.2. Updated/amended authorisation ☐

4.3. renewed authorisation ☐ 4.4. EU Identification Number of the previous Safety Authorisation _____

4.5. The applying infrastructure manager operates freight wagons to transport materials for construction or for infrastructure maintenance activities: YES/NO

The applying infrastructure manager belongs to the following categories for estimated number of employees

4.6. Micro enterprise ☐ 4.8. Medium sized enterprise ☐

4.7. Small enterprise ☐ 4.9. Large enterprise ☐

IF THE APPLICANT ALREADY HOLDS A VALID SAFETY AUTHORISATION IT SHOULD PROVIDE THE FOLLOWING INFORMATION

5.1. EU Identification Number of Safety Authorisation _____

SUBMITTED DOCUMENTS

6.1. ☐ Summary of the manual of the Safety Management System as referred to in Art. 9 and Annex III of Directive 2004/49/EC

6.2. ☐ Other (specify)

_____

Applicant _____
(first name, family name)

Date _____ Signature _____

Internal reference number

_____ Date application received _____

SPACE RESERVED FOR THE ADDRESSED OFFICE/AUTHORITY

Annex 2 Standard format for safety authorisation[27]

SAFETY AUTHORISATION

Safety Authorisation confirming acceptance of the Safety Management System within the European Union in conformity with Directive 2004/49/EC and applicable national legislation

EU IDENTIFICATION NUMBER:

1. AUTHORISED INFRASTRUCTURE MANAGER

Legal denomination:	
Infrastructure Manager name:	Acronym:
National registration number:	VAT No:

2. ORGANISATION ISSUING AUTHORISATION

Organisation:
Country:

3. AUTHORISATION INFORMATION

This is a - new authorisation ☐ - renewed authorisation ☐ - updated/amended authorisation ☐	ECM (entity in charge of maintenance) certificate: YES/NO ECM certificate number: EU Identification Number of the previous authorisation:
Validity from:	to:
Particulars of Infrastructure(s):	
Infrastructure Manager size:	
Scope of ECM activities: Covers tank wagons for dangerous goods: YES/NO Covers other wagons specialised in transport of dangerous goods: YES/NO	

[27] *This format is not prescribed by EU legislation but recommended for use.*

4. APPLICABLE NATIONAL LEGISLATION

5. ADDITIONAL INFORMATION

Date issued

Signature

Internal reference number

Authority's stamp

Annex 3 Case study examples

1. The emergency department of an IM uses specialised and motorised vehicles, which are transported with a van over the road and then placed on the rail to intervene where the accident occurred. The IM has neither a safety certificate nor a licence.

   Should the IM be considered as RU and then, apply for a safety certificate?

The use of such vehicles does not change the principal activity (or business) of the IM to provide transport of goods and/or passengers by rail. The technical specification of interoperability relating to the "operation and traffic management" subsystem of the rail system in the European Union (TSI OPE) sets the requirement for the IM to establish specific measures to manage emergency situations together with the RUs or representatives of the RUs which shall be then included in the SMS of the IM (and the RUs).

As follows, since in this case the IM is not considered as an RU, it shall not obtain any safety certificate. Neither it shall be licensed according to Directive 2012/34/EU (previously Directive 95/18/EC) as its principal business has not changed to transport of goods/passengers. It shall hold a safety authorisation.

In the course of the assessment of conformity of the IM's SMS, the processes for managing an emergency situation should have been under scrutiny. The NSA could then assess the existence of the necessary provisions to control the risks of these activities in the IM's SMS.

The above case and related conclusion can also be expanded to the question regarding the situation where the IM uses subcontractors, e.g. to transport materials for maintenance tasks or to project sites when building new lines.

2. An international RU operates on the infrastructure of a neighbouring Member State not beyond the first station located after the state border.

   Should a Part B safety certificate still be granted to the international company?

   This RU plans to operate in another neighbouring Member State and applies for a safety certificate (Part B) to the NSA of that Member State whereas the RU does not know yet when its operation will start.

   Should the NSA of the neighbouring Member State grant a Part B safety certificate for a railway company that has not yet started any operation in its Member State and that does not know when it will be able to start its operation? How can it be controlled by the NSAs of both neighbouring Member States?

Article 10.2(b) of Directive 2004/49/EC (the Railway Safety Directive) requires an RU to obtain a network specific safety certificate (Part B) from the NSA in the Member State it wishes to operate in, after it has obtained a Part A safety certificate valid throughout the European Union. So, a RU operating in the neighbouring Member State should apply for a safety certificate in relation to conducting its operations in the neighbouring Member State.

If an RU operates until the 'frontier' location(s), i.e. any location(s) designated as the 'frontier' in the network statement of an IM and included in its safety authorisation (e.g. the first station beyond the border), then it should already have demonstrated the capability to meet the network specific requirements (whilst the network (or parts of it) extends physically beyond the geographical border of a neighbouring MS as part of cooperation arrangements between IMs) and therefore have already been granted a domestic Part B safety certificate covering also the frontier location (see section 3.1.2). Those network specific requirements should be included in the network statement of the IM allocating the infrastructure capacity (see Annex IV of Directive 2012/34/EU). Under the above conditions, provided that both neighbouring MS decide so, the RU may not be required to apply for a Part B safety certificate to the NSA of the neighbouring Member State.

The Part B safety certificate can be granted to the applicant if it complies with the assessment criteria of the CSM Regulation for Conformity Assessment 1158/2010/EU. However, pursuant to Article 10(5) of the RSD, the NSA must revoke a safety certificate if it is apparent that the holder of the safety certificate has not used it as intended[28] in the year following its issue. Furthermore, as soon as this RU makes a decision to (effectively) operate in the other Member State to which it applied for the Part B safety certificate, the NSA of this Member State shall conduct at the earliest opportunity relevant supervision activities. Pursuant to Article 9(4) of the RSD, the RU shall submit to the NSA an annual safety report. The RU shall submit this report to the concerned Member States for their respective part (i.e. information related to the Part A and Part B for the first Member State where the RU is registered, and to the Part B for the second Member State).

3. Business arrangements (e.g. joint venture agreement) exist between railway undertakings whereby the railway operation (e.g. passenger traffic), including traction, in a Member State MS1 by an "international" RU (i.e. registered in another Member State MS2) are covered by the safety certificate Parts A and B of an "incumbent" RU in MS1; the "international" RU being subcontractor of the "incumbent" RU.

   The Part A safety certificate of the "incumbent" RU covers the way it arranged the distribution of the safety tasks with its subcontractors and its monitoring of the delegated safety tasks.

   The Part B of the "incumbent" RU in MS1 covers in particular how it accepts the rolling stock and the safety personnel from its sub-contractors, as the "international" RU, but also the practical arrangements for the exchange of documentation and information.

   Should the international RU apply for a Part B safety certificate in MS1, the Member State of the "incumbent" RU? Who is providing "traction"? Which company is responsible for the safe operation?

The safety certificate is the evidence that the "incumbent" RU has established its SMS and therefore has put in place the necessary arrangements to manage and control all risks associated with its activity in MS1.

The fact that the SMS of the "incumbent" RU covers the operation of its subcontractors in MS1 means that such subcontractors do not operate as an RU for the operation concerned by the cooperation in that MS. It is therefore an obligation for the "incumbent" RU to check that their contractors comply

[28] *For the same type and extent of operation.*

with all applicable laws in MS1. The fact that the "incumbent" RU accepts all potential liabilities resulting from the activities of its subcontractors in MS1 supposes it has identified all the subcontracted activities and enforces, by means of a contract, the resulting obligations for these subcontractors.

The "incumbent" RU is the one having the responsibility for coordinating and managing the safe running of the train, it therefore needs to hold a safety certificate for the operations in MS1.

The contracting "incumbent" RU has the responsibility, as part of its SMS, to clearly specify in the contract what it requires the subcontractor to do and the quality of the outputs it expects the subcontractor to deliver, as well as to monitor the outputs of the subcontractor to make sure it meets the original specification in the contract. The sub-contracted RU should cover the operational elements in their SMS and both should have effective co-operation and co-ordination arrangements.

The partner, as an "international" RU, having a safety certificate in MS2 may help the "incumbent" RU who subcontracts operations in MS1 to gain confidence, but it is not a prerequisite for subcontracting. Taking into account the "international" RU's safety certificate allows the "incumbent" RU to relax the control process by relying on the "international" RU's practical experience in his country and on the controlled and monitored processes in its SMS. Consideration for the partner's hierarchical organisation and processes (e.g. staff roster and continuous training), which are described in its SMS, may limit or avoid interference in its day-to-day operations, provided the "incumbent" RU gives the necessary information and performs regular checks and audits.

If the "incumbent" RU takes over, through contractual arrangements, the operation of a train from the "international" RU when the train enters into the territory of the MS1 where the "incumbent" RU operates, then each RU can operate the same train on the network of the Member State where it has obtained its part B safety certificate, i.e. the "incumbent" in MS1 and the "international" RU in MS2.

To conclude:

- Neither Part A nor Part B safety certificates of the "incumbent" RU can be used by another RU who supplies traction (i.e. the use of locomotive(s) and train driver(s)). The "incumbent" RU has the responsibility for coordinating and managing the safe running of trains on the network where it operates, even when subcontracting activities.
- RU can only operate on a network, and thereby is responsible for its safe operation, if it has a valid Part A and Part B safety certificate, irrespective of its contractual arrangements concluded with other RUs or other legal entities concerning its operation.
- Hence, the railway operations of "international" RUs in a Member State which are subcontractors of the "incumbent" RU of that Member State must be controlled by the "incumbent" RU who must have processes in its SMS to define and control activities performed by the subcontractor. Part A of the safety certificate covers the way it arranged the distribution of the safety tasks with its subcontractors and its monitoring of the delegated safety tasks, and Part B of the safety certificate covers how it accepts the rolling stock and the safety personnel from its sub-contractors and the practical arrangements for the exchange of documentation and information. **Responsibilities for safety and the obligations to have a safety certificate may not depart in the contractual arrangements from the basic principles laid down in the RSD**.

The above case and related principles and conclusion could also apply to joint venture agreementsbinding two companies registered in two different neighbouring Member States where train composition mixes locomotives and wagons from both companies and the train crew is changed over at the border.

Annex 4 Examples of good cooperation practices between Railway Undertakings

This Annex presents good co-operation practices between partner Railway Undertakings focusing on:

a) How risk can be controlled within the scope of partnerships;

b) The nature of agreements for the procurement of services, e.g. traction, traction manager, maintenance of the rolling stock.

In accordance with Article 4 of RSD and Annex II of CSM Regulation on Conformity Assessment 1158/2010/EU, the RU has to manage the risks of its operations, including those related to partnerships. The operations have to satisfy the European and national legal requirements and the internal standards of the RU.

All definitions of responsibility and tasks are to be defined in the respective contracts. The task delivery is integrated into the operational processes of the partner companies.

This can be reached by (not limited to):

- Stating clear contractual provisions (Cf. criteria C.2 to C.4) including:
  - A description of the task(s) and output(s) to be delivered;
  - The expected quality of the output(s);
  - The assignment of roles and responsibilities;
  - Communication protocols, i.e. what, when and how information will be exchanged between the contractual parties. Information includes reporting on events and sharing of experience;
  - Competence requirements for the staff involved in delivering the task;
  - Health and safety requirements (deriving from risk assessment, national requirements, etc.);
  - Monitoring requirements, e.g. supplier audits, to check that the output has been delivered and meets the original specification.
- Establishing communication protocols with identification of reporting lines and sharing safety relevant information between involved parties, e.g. any operational restrictions imposed by the IM (Cf. criterion O);
- Assigning clear roles and responsibilities in the SMS (Cf. criterion F);
- Delivering the train driver's certificate to operate the train on the infrastructure (Cf. criterion N);
- Ensuring other train crew are suitably trained and have required competence (Cf. criterion N);
- Implementing risk identification and risk control measures (Cf. criteria A, M);
- Setting adequate monitoring procedures based on contractual arrangements, e.g. sufficient communication controls in place to manage the operation (Cf. criteria C.5 and N.2, CSM Regulation on monitoring 1078/2012/EU).
- Specific procedures are to be implemented within the SMS of the partner companies that describe in detail:
  - How the scope of the cooperation is defined and which operational roles need to be involved;
  - Who is responsible to define necessary contractual agreements and additional documents;
  - Who is responsible to distribute necessary rules and standards (related to personnel and rolling stock); and

- How and (respectively) by whom the interfaces are managed and monitored.

Annex II of CSM Regulation for Conformity Assessment 1158/2010/EU also requires specific procedures to be defined for controlling the risks related to the use of contractors (Cf. criteria C.1 to C.5):

C.1 - "There are procedures to verify the competence of contractors (including subcontractors) and suppliers"

Subcontracting will be easier with a company already having a safety certificate (e.g. for international traffic). The safety certificate is the cornerstone for building mutual trust and reliance on a partner's practical experience in its country and in its SMS (monitored and controlled) processes.

C.2 - "There are procedures to verify and control the safety performance and results of all contracted services and products supplied either by the contractor or supplier to ensure that they comply with the requirements set out in the contract"

In the following example, i.e. a driver of RU "X" operating rolling stock of RU "X" in a neighbouring country (other than the one where the RU "X" is registered) as subcontractor of RU "Y", the monitoring and checks can be based on:

- continuous training targets established in common on a yearly basis
- transfer of information (including reporting of events and return of experience on incidents), RU "X" informing RU"Y" in case of any problem (signal passed at danger, overspeed etc.) under a predefined format
- cross-verifications and audits
- safety review (e.g. once a year) and ad-hoc review if any change
- change management (e.g. specific training needed in case of new regulation in force, new route or new rolling stock)
- communications arrangements between the parties involved

C.3 - "Responsibilities and tasks relating to railway safety issues are clearly defined, known and allocated between the contracting partners and among all other interested parties":

In the above example, the driver's training and the monitoring of the competency over time can be managed as follows:

- The RU "X" trainers, examiners and supervisors are recognised by the RU "Y" that checks knowledge, skills and aptitudes
- Qualification is carried out by the RU "X" examiner authorised/recognised by the RU "Y"
- The train drivers certificate is issued by the RU "X" on behalf of the RU "Y" (for specific routes RU "Y" operates on)
- Continuous follow-up of competency performed by the RU "X" through its own SMS processes

C.4 - "There are procedures to ensure traceability of safety-related documents and contracts"

In the above example:

- Records of supervision of a train driver of a partner operating on behalf of the RU "Y"
- Assessments to monitor success of continuous training of a train driver of a partner operating on behalf of the RU "Y"

C.5 - "There are procedures to ensure that safety tasks, including the exchange of safety-related information, are performed by the contractors or the supplier according to relevant requirements set out in the contract"

In the above example:

- Documentation: The rulebook is limited by the RU "Y" to the specific activities and missions to be performed by RU "X" drivers, e.g. translation is made by an interpreter (in the mother language of RU "X") under RU "Y" control and validated by a group of RU "X" and RU "Y" experts
- Individual licences for drivers are valid in the whole EU; linguistic level is set in Directive 2007/59/EC. The linguistic level can be checked by an independent institution (e.g. university) whilst the railway specific terminology is defined by the RU "Y"
- Training is performed in the train driver's mother tongue, except for drills which may be performed in the IM's language, but under the responsibility and supervision of a recognised training centre of the RU "Y" (or a certified trainer working under the responsibility of the recognised training centre)

The safety certificate issued by the partner's NSA can be accepted as proof of the ability of the partner to meet the requirements governing the use of contractors specified in Annex II, criteria C.2 to C.4, to CSM Regulation for Conformity Assessment 1158/2010/EU.

Annex 5 References and abbreviations

Table 3 : Table of references

[Ref. N°]	*Title*	*Reference*	*Version*
[1]	Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licencing of railway undertakings and Directive 2011/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive)	OJ L 220, 21.6.2004, p.16	-
[2]	Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the Interoperability of the rail system within the Community	OJ L 191, 18/7/2008, p.1.	-
[3]	Commission Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009	OJ L 121, 3.5.2013, p. 8–25	-
[4]	Commission Regulation (EU) No 1158/2010 on a common safety method for assessing conformity with the requirements for obtaining railway safety certificates	OJ L 326, 10.12.2010, p. 11-24	-
[5]	Commission Regulation (EU) No 1169/2010 on a common safety method for assessing conformity with the requirements for obtaining a railway safety authorisation	OJ L 327, 11.12.2010, p. 13-25	-
[6]	Commission Regulation (EU) No 1077/2012 on a common safety method for supervision by national safety authorities after issuing a safety certificate or safety authorisation	OJ L 320, 17.11.2012, p. 3–7	-
[7]	Commission Regulation (EU) No 1078/2012 on a common safety method for monitoring to be applied by railway undertakings, infrastructure managers after receiving a safety certificate or safety authorisation and by entities in charge of maintenance	OJ L 320, 17.11.2012, p. 8–13	-
[8]	Commission Recommendation (EU) No 2014/897 on matters related to the placing in service and use of structural subsystems and vehicles under Directives 2008/57/EC and 2004/49/EC of the European Parliament and of the Council	OJ L 355, 12.12.2014, p. 59–77	-
[9]	ERA guidance – Common approach to supervision of railway undertakings operating in more than one Member State	ERA/GUI/12-2013/SAF	1.0

Table 4 : Table of abbreviations

Abbreviation	*Meaning*
CA	Conformity Assessment
CSM	Common Safety Method
EC	European Commission
ECM	Entities in Charge of Maintenance
ERA	European Railway Agency
EU	European Union
IM	Infrastructure Manager
MS	Member State
NSA	National Safety Authority
RSD	Railway Safety Directive [1]
RU	Railway Undertaking
SA	Safety Authorisation
SC	Safety Certification
SMS	Safety Management System

Annex 6 Safety assessment forms

Annex 6.1 First Screen Form

First Screen Form					
Applicant *(legal denomination)*		**Date of application**		**File Ref. No**	
Type of application *(SC Part A/SC Part B/SA)*		**Assessor(s)**		**Accountable Manager**	

Application form (Cf. Annex III of Reg. (EC) 653/2007)		**Y/N**	**Comments**
a) Appropriate boxes ticked? (including front pages for annexes to the application form)			
b) Consistent with type and extent of the operation as described in the application dossier?[29]			
Type	**Documents to be submitted**	**Complete (Y/N)**[30]	**Comments**
SC Part A	Summary of the manual of the Safety Management System as referred to in Art. 9 and Annex III of Directive 2004/49/EC The SMS manual should be supplemented by an overall description of the following (if not already included in the above manual): - the type and extent of railway operations		

[29] *If the applicant selects the tick-boxes for a type and extent of service, e.g. freight operation with dangerous goods, then the application dossier shall entail related documents.*
[30] *Specify 'N/A' (Not Applicable) for elements of the list not dovetailing the type of application.*

	- the type and level of safety risks the organisation is exposed to - the monitoring strategy and plan as referred to in Regulation (EU) n°1078/2012 - how the Safety Management System is used and implemented by managers - how continuous improvement is achieved - how responsibilities are distributed - the document management system - the competence management system - the information management system		
	Copy of the Licence (if applicable)		
SC Part B	Copy of the Part A Certificate		
	Copy of the Licence (if applicable)		
	Copy of insurance or financial cover for liability, annexed to the Licence		
	List of necessary rules and TSI's with reference to the processes in the Safety Management System and documents how they are implemented		
	List of different categories of staff, either employed or contracted		
	Description of staff related processes of the Safety Management System required by national rules or TSI's and reference to the national relevant certificates where necessary		
	List of different types of rolling stock		
	Description of rolling stock related processes in the Safety Management System required by national rules or TSI's and reference to the national relevant certificates where necessary		

	Other		
SA	Summary of the manual of the Safety Management System as referred to in Art. 9 and Annex III of Directive 2004/49/EC The SMS manual should be supplemented by an overall description of the following (if not already included in the above manual): - the type and extent of railway operations - the type and level of safety risks the organisation is exposed to - the monitoring strategy and plan as referred to in Regulation (EU) n°1078/2012 - how the Safety Management System is used and implemented by managers - how continuous improvement is achieved - how responsibilities are distributed - the document management system - the competence management system - the information management system		
	Other		

Further information requested?	*(Y/N)*	**Date of receipt of supplementary information[31]**	*(DD/MM/YY)*

Is the application complete?	*(Y/N)*

[31] *If any supplementary information is requested several times from the applicant, it should be specified the respective dates of receipt.*

Name of the responsible person	*(First name, surname)*
Date and signature	

Annex 6.2 Initial Review Form (Railway Undertaking)

Initial Review Form			
Applicant *(legal denomination)*		**Assessor(s)**	

Initial Review: Sufficient evidence for assessment - you should check that evidence is provided against the **main** requirements of each relevant criterion (as summarised in the table below) and that the evidence is clearly structured and presented. Although this is a simple 'yes/no' exercise, comments fields are provided which may be used to make brief notes to assist with the later detailed assessment.

Criteria	**Y/N**		**Criteria**	**Y/N**	
Risk control measures for all risks (A)		**Comments**	**Risk control for the supply of material and maintenance (B)**		**Comments**
Procedures to identify risks.			Maintenance requirements, standards and processes derived from data.		
Procedures for risk control measures.			Maintenance intervals adapted according to type and extent of service.		
Procedures to monitor measures and implement changes.			Maintenance responsibilities clearly defined.		
Arrangements to work with other entities in place.			Information on malfunctions and defects collected and reported		
Documentation and communication method agreed between entities.			Risks from defects and construction malfunctions reported to appropriate parties.		

Arrangements monitored and changes can be made if needed.			Maintenance is controlled and verified to comply with corporate standards.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Risk control of contractors and suppliers (C)		**Comments**	**Risks arising from parties external to the railway system (D)**		**Comments**
Contractors and suppliers competence verified?			Potential risks from external parties identified where appropriate and reasonable.		
Safety performance and results verified and controlled in line with contract?			Control measures can be established for the risks identified.		
Railway safety responsibilities and tasks clearly defined, known and allocated between parties?			Procedures to monitor the effectiveness of the control measures are in place.		
Safety documents and contracts are traceable.					
Safety tasks including information exchange meets the contract requirements.					
Criteria	**Y/N**		**Criteria**	**Y/N**	
Documentation of the safety management system (E)		**Comments**	**Distribution of responsibilities (F)**		**Comments**
Description of the activity that states type, extent and risk of operation			Description of how coordination of SMS activities is ensured across organisation.		

Description of the SMS including allocation of roles and responsibilities			Authority, competence and appropriate resources are given to staff with delegated responsibilities.		
Description of SMS procedures consistent with type and extent of services.			Safety related responsibilities and their distribution to specific functions are defined		
Safety critical processes and tasks are listed and described			Safety tasks are defined and delegated to competent staff		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Securing control by management on different levels (G)		**Comments**	**Involving staff and their representatives at all levels (H)**		**Comments**
Responsibilities are allocated for each safety related process.			Procedure to ensure staff and their representatives are consulted on the safety aspects of operational procedures.		
Procedure for monitoring task performance and how management will intervene on poor performance			Staff involvement and consultation arrangements are documented.		
Procedure to identify management activities and manage their impact on the SMS.					
Procedure to hold managers of safety accountable for their performance					
Procedure to allocate resources to deliver SMS tasks					
Criteria	**Y/N**		**Criteria**	**Y/N**	

Ensuring continuous improvement (I)		**Comments**	**Safety policy (J)**		**Comments**
Procedure in place to ensure continuous improvement of SMS.			Safety policy exists, is approved by Chief Executive and communicated to all staff.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Qualitative and quantitative targets for maintaining and enhancing safety (K)		**Comments**	**Existing, new and altered technical and operational standards or other prescriptive conditions (L)**		**Comments**
Relevant safety targets are set and documented in line with legal obligations.			Safety requirements identified and reflected in procedures & updated when changes made, implemented and monitored. Actions taken where non-compliance is found.		
The targets are consistent with type and extent of operations and risks.			Procedures to ensure staff, procedures, equipment and rolling stock are used for the intended purpose.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Qualitative and quantitative targets for maintaining and enhancing safety (K) cntd		**Comments**	**Existing, new and altered technical and operational standards or other prescriptive conditions (L) cntd**		**Comments**
Overall safety performance is assessed against targets.			SMS ensures maintenance is carried out to relevant requirements		
Procedures to regularly monitor and review operational arrangements are in place.					
RU has developed procedures and plans to meet its targets.					
Criteria	**Y/N**		**Criteria**	**Y/N**	

Procedures and methods for evaluating new risks and implementing control measures (M)		**Comments**	**Staff training programmes and systems to maintain competence (N)**		**Comments**
Management procedures for changes in equipment, procedures, organisation staffing and interfaces.			CMS includes identification of knowledge and skills, selection principles, initial and ongoing training, checks of competence, special measures as required and SMS training.		
Changes are managed by applying the CSM on risk evaluation and assessment.			CMS procedures include identification of posts that perform safety tasks; make operational decisions; staff having the necessary knowledge, skills, competence and aptitude for their tasks; and monitoring staff performance and taking corrective actions.		
Results of risk assessment are fed into other organisational processes and are visible to staff.					
Criteria	**Y/N**		**Criteria**	**Y/N**	
Provision of information within organisation and between those operating on the same infrastructure (O)		**Comments**	**Documenting and controlling safety information (P)**		**Comments**
Staff knows and understands the SMS and can access information/documents on it.			Safety information is accurate, complete, consistent, understandable, up-to-date and documented.		
Staff is aware of and has access to key operational information before it needs to be applied.			Procedures allow safety information to be formatted, generated, distributed		

			and managed and received collected and stored.		
Information is shared between organisations			Procedure for layout control of vital safety information.		
Accidents, incidents, near misses and other DOs (Q)		**Comments**	**Emergencies: Provision for plans of action, alerts and information (R)**		**Comments**
All incidents reported as required. They are logged investigated and analysed			All types of emergency are documented and procedures to identify any new ones are in place. Roles and responsibilities are set out in the document.		
Recommendations from investigations are evaluated and implemented where required.			Emergency services have the necessary information to prepare their response and deal with the emergency. They can be promptly contacted.		
Information on the investigation and causes of incidents is used to learn and adopt preventative measures			Plans of action, alerts and information include: procedures to alert emergency management staff; arrangements to communicate including passengers.		
			Resources and means have been allocated, training needs identified and documented.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Accidents, incidents, near misses and other DOs (Q) cntd		**Comments**	**Emergencies: Provision for plans of action, alerts and information (R) cntd**		**Comments**
			Emergency plans have been tested to train staff, identify weak points and check how potential emergencies are managed. They are coordinated with		

			railway undertakings which operate on the infrastructure.		
			There is a procedure to contact entities in charge of maintenance or the railway vehicle keeper in an emergency. There are procedures to restart normal operating conditions as soon as possible.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
SMS: Recurrent internal auditing. (S)		**Comments**	**Compliance with network-specific rules (Part B - A)**		**Comments**
Independent and impartial internal auditing system in place that acts transparently.			Network specific rules and risks have been identified and can be complied with and/or exceptions/derogations shown		
Schedule of planned internal audits, revised based on previous audits and performance is in place.			Network interfaces with all others involved in the operation of the railway have been identified.		
Suitably competent auditors identified and selected.			How RUs will interact, and share information, with the IM and other RUs is documented.		
Audits are analysed, evaluated, and recommend follow up measures. The effectiveness of the execution and results of audits are checked and documented.			How the RU will deal with emergencies including coordination with IM and public authorities is documented.		
Senior managers know the result of audits and are responsible for changes to the SMS			Specific incident/accident investigation rules are documented and can be complied with.		

Criteria	Y/N		Criteria	Y/N	
SMS: Recurrent internal auditing. (S) cntd		**Comments**			
How audits are planned with routine monitoring ensures compliance with internal procedures and standards					
Criteria	**Y/N**		**Criteria**	**Y/N**	
Compliance with network-specific staff competence requirements. (Part B - B)		**Comments**	**Compliance with network-specific management of rolling stock requirements (Part B - C)**		**Comments**
The documented SMS contains a CMS which identifies categories of staff and delivers competent staff for the network.			Types of rolling stock used, including any operational restrictions, and operations to be conducted are clearly documented.		
Staff's day to day work is organised to ensure they are carrying out appropriate tasks and safety-related tasks are done.			Any identified additional maintenance requirements and appropriate arrangements are documented and in place.		
Documents used in training relevant staff are accurate, kept up to date and understandable by staff.			Any additional requirements to manage rolling stock incidents are identified, documented and in place.		

Is there sufficient evidence to carry out an assessment?	Yes ☐ No ☐
Is the evidence clearly structured and presented?	Yes ☐

		No ☐	
If answering 'no' in either or both the above does the applicant need to be asked to re-submit?		Yes ☐ No ☐	
Does further information need to be requested?		Yes ☐ No ☐ (If yes summarise details) *…press 'enter' to extend*	
Date of completion of Initial Review		**Assessor(s) signature**	

If re-submission of the application is required, the accountable manager should confirm this.			
I confirm that the applicant should be asked to re-submit their application			
Accountable manager's signature		**Date**	

Annex 6.3 Initial Review Form (Infrastructure Manager)

Initial Review Form			
Applicant *(legal denomination)*		**Assessor(s)**	

Initial Review: Sufficient evidence for assessment - you should check that evidence is provided against the main requirements of each relevant criterion (as summarised in the table below) and that the evidence is clearly structured and presented. Although this is a simple 'yes/no' exercise, comments fields are provided which may be used to make brief notes to assist with the later detailed assessment.

Criteria	**Y/N**		**Criteria**	**Y/N**	
Risk control measures for all risks (A)		**Comments**	**Risk control for the supply of material and maintenance (B)**		**Comments**
Procedures to identify risks.			Maintenance requirements, standards and processes derived from data.		
Procedures for risk control measures.			Maintenance intervals adapted according to type and extent of service.		
Procedures to monitor measures and implement changes.			Maintenance responsibilities clearly defined.		
Arrangements to work with other entities in place.			Information on malfunctions and defects collected and reported		
Documentation and communication method agreed between entities.			Risks from defects and construction malfunctions reported to appropriate parties.		

Arrangements monitored and changes can be made if needed.			Maintenance is controlled and verified to comply with corporate standards.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Risk control of contractors and suppliers (C)		**Comments**	**Risks arising from parties external to the railway system (D)**		**Comments**
Contractors and suppliers competence verified?			Potential risks from external parties identified where appropriate and reasonable.		
Safety performance and results verified and controlled in line with contract?			Control measures can be established for the risks identified.		
Railway safety responsibilities and tasks clearly defined, known and allocated between parties?			Procedures to monitor the effectiveness of the control measures are in place.		
Safety documents and contracts are traceable.					
Safety tasks including information exchange meets the contract requirements.					
Criteria	**Y/N**		**Criteria**	**Y/N**	
Documentation of the safety management system (E)		**Comments**	**Distribution of responsibilities (F)**		**Comments**
Description of the activity that states type, extent and risk of operation			Description of how coordination of SMS activities is ensured across organisation.		

Description of the SMS including allocation of roles and responsibilities			Authority, competence and appropriate resources are given to staff with delegated responsibilities.		
Description of SMS procedures consistent with type and extent of services.			Safety related responsibilities and their distribution to specific functions are defined		
Safety critical processes and tasks are listed and described			Safety tasks are defined and delegated to competent staff		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Securing control by management on different levels (G)		**Comments**	**Involving staff and their representatives at all levels (H)**		**Comments**
Responsibilities are allocated for each safety related process.			Procedure to ensure staff and their representatives are consulted on the safety aspects of operational procedures.		
Procedure for monitoring task performance and how management will intervene on poor performance			Staff involvement and consultation arrangements are documented.		
Procedure to identify management activities and manage their impact on the SMS.					
Procedure to hold managers of safety accountable for their performance					
Procedure to allocate resources to deliver SMS tasks					
Criteria	**Y/N**		**Criteria**	**Y/N**	
Ensuring continuous improvement (I)		**Comments**	**Safety policy (J)**		**Comments**

Procedure in place to ensure continuous improvement of SMS.			Safety policy exists, is approved by Chief Executive and communicated to all staff.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Qualitative and quantitative targets for maintaining and enhancing safety (K)		**Comments**	**Existing, new and altered technical and operational standards or other prescriptive conditions (L)**		**Comments**
Relevant safety targets are set and documented in line with legal obligations.			Safety requirements identified and reflected in procedures & updated when changes made, implemented and monitored. Actions taken where non-compliance is found.		
The targets are consistent with type and extent of operations and risks.			Procedures to ensure the staff, documents, equipment and rolling stock are used for the intended purpose.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Qualitative and quantitative targets for maintaining and enhancing safety (K) continued		**Comments**	**Existing, new and altered technical and operational standards or other prescriptive conditions (L) continued**		**Comments**
Overall safety performance is assessed against targets.			SMS ensures maintenance is carried out to relevant requirements		
Procedures to regularly monitor and review operational arrangements are in place.					
IM has developed procedures and plans to meet its targets.					
Criteria	**Y/N**		**Criteria**	**Y/N**	
Procedures and methods for evaluating new risks and		**Comments**	**Staff training programmes and systems to maintain competence (N)**		**Comments**

implementing control measures (M)					
Management procedures for changes in equipment, procedures, organisation staffing and interfaces.			CMS includes identification of knowledge and skills, selection principles, initial and ongoing training, checks of competence, special measures as required and SMS training.		
Changes are managed by applying the CSM on risk evaluation and assessment.			CMS procedures include identification of posts that perform safety tasks; make operational decisions; staff having the necessary knowledge, skills, competence and aptitude for their tasks; and monitoring staff performance and taking corrective actions.		
Results of risk assessment are fed into other organisational processes and are visible to staff.					
Criteria	**Y/N**		**Criteria**	**Y/N**	
Provision of information within organisation and between those operating on the same infrastructure (O)		**Comments**	**Documenting and controlling safety information (P)**		**Comments**
Staff knows and understands the SMS and can access information/documents on it.			Safety information is accurate, complete, consistent, understandable, up-to-date and documented.		
Staff is aware of and has access to key operational information before it needs to be applied.			Procedures allow safety information to be formatted, generated, distributed and managed.		
Information is shared between organisations			Procedure for layout control of vital safety information.		

Criteria	Y/N		Criteria	Y/N	
Accidents, incidents, near misses and other DOs (Q)		**Comments**	**Emergencies: Provision for plans of action, alerts and information. (R)**		**Comments**
All incidents reported as required. They are logged investigated and analysed			All types of emergency are documented and procedures to identify any new ones are in place. Roles and responsibilities are set out in the document.		
Recommendations from investigations are evaluated and implemented where required.			Emergency services have the necessary information to prepare their response and deal with the emergency. They can be promptly contacted.		
Information on the investigation and causes of incidents is used to learn and adopt preventative measures			Plans of action, alerts and information include: procedures to alert emergency management staff; arrangements to communicate including passengers.		
			Resources and means have been allocated, training needs identified and documented.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Accidents, incidents, near misses and other DOs (Q) cntd		**Comments**	**Emergencies: Provision for plans of action, alerts and information. (R) cntd**		**Comments**
			Emergency plans have been tested to train staff, identify weak points and check how potential emergencies are managed. They are coordinated with railway		

			undertakings which operate on the infrastructure.		
			Operations and railway traffic can be stopped promptly and interested parties informed of the action. There are procedures to restart normal operating conditions as soon as possible.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
SMS: Recurrent internal auditing. (S)		**Comments**	**Safe design of the railway infrastructure (T)**		**Comments**
Independent and impartial internal auditing system in place that acts transparently.			Procedures to ensure safe design and installation of the infrastructure throughout its lifecycle are in place.		
Schedule of planned internal audits, revised based on previous audits and performance is in place.			Procedures to manage a technical change in the infrastructure are in place.		
Suitably competent auditors identified and selected.			Procedures on the relevant rules about design of the infrastructure and national safety methods have been identified and can be complied with.		
Audits are analysed, evaluated, and recommend follow up measures. The effectiveness of the execution and results of audits are checked and documented.					
Criteria	**Y/N**		**Criteria**	**Y/N**	
SMS: Recurrent internal auditing. (S) cntd		**Comments**			

Senior managers know the result of audits and are responsible for changes to the SMS					
How audits are planned with routine monitoring ensures compliance with internal procedures and standards					
Criteria	**Y/N**		**Criteria**	**Y/N**	
Safe operation of the infrastructure. (U)		**Comments**	**Provision of maintenance and material (V)**		**Comments**
Procedures ensure the infrastructure is managed and operated safely.			Procedures ensure safe maintenance of the Infrastructure, including clear management control and documented audit.		
Procedure shows how infrastructure is operated safely at physical/operational borders.			Maintenance of the infrastructure meets the needs of the network.		
Criteria	**Y/N**		**Criteria**	**Y/N**	
Safe operation of the infrastructure. (U) cntd		**Comments**	**Provision of maintenance and material (V) cntd**		**Comments**
Procedure for how effective cooperation and coordination is managed normally and in emergency.			Rules about the supply of maintenance and material have been identified and are complied with		
Rules about safe operation and management of infrastructure/vehicle interfaces have been identified and are complied with					

Criteria	Y/N				
Maintenance and operation of the traffic control and signalling system. (W)		**Comments**			
Procedure ensure that the traffic control and signalling system is safely operated and maintained.					
Procedures ensure compliance with existing, new or altered technical and operational standards					
Safety at the physical/operational borders of the system is properly managed.					
Rules about the safe operation and management of the system have been identified and complied with.					

Is there sufficient evidence to carry out an assessment?	Yes ☐ No ☐
Is the evidence clearly structured and presented?	Yes ☐ No ☐
If answering 'no' in either or both the above does the applicant need to be asked to re-submit?	Yes ☐ No ☐

Does further information need to be requested?		Yes ☐ No ☐ (If yes summarise details) *…press 'enter' to extend*	
Date of completion of Initial Review		**Assessor(s) signature**	

If re-submission of the application is required, the accountable manager should confirm this.			
I confirm that the applicant should be asked to re-submit their application			
Accountable manager's signature		**Date**	

Annex 6.4 Assessment Form

Assessment Form			
Applicant *(legal denomination)*		**File Ref. No**	
Assessor(s)		**Accountable Manager**	

Part 1: Compliance with Assessment Criteria *(This part of the form is to be sent to the applicant)*	
List the criteria which have been complied with (give designation and number, e.g. RU-A)	…tab to extend

For those where compliance is <u>not</u> complete or fully apparent provide details below

Ref. No. *(Initials followed by sequential no.)*	**Document section/** **page/paragraph**	**Criterion No. /Reg.**	**Details (e.g. lack of information, lack of clarity)** **Subject** **Comments** **Action required**	**Applicant's response**	**Outcome** *(Closed out or supplementary matter raised)* *(Date of closure or suppl. ref. no.)* *(Comments on applicant's response)*

					…tab to add rows

Part 2: Matters to be considered for supervision	
The following matters warrant early supervision to ensure that the arrangements described in the application are fully implemented.	**The following matters should be considered for inclusion in later supervision**
	…tab to add rows

Part 3: Assessor's conclusion *(This section should only to be completed after all necessary further information has been received; If several assessors, Lead Assessor is asked to draft the conclusion)*

I have assessed all topics assigned to me and I consider that the issues I have raised have been/ have not been* satisfactorily closed out (if not satisfactory, give reasons above) (*delete as appropriate) Also please use the space above to make any comment on the overall quality of the application.			
Assessor(s) signature		**Date**	

Annex 6.5 Assessment Report

Assessment Report			
Applicant *(legal denomination)*		**File Ref. No**	
Assessor(s)		**Accountable Manager**	
Purpose and scope of the assessment			
History of the assessment			

Part A *(Tables 1-4: to be completed by the assessor(s) and forwarded to the Accountable Manager)*		
Table 1: The application has complied with all relevant assessment criteria/There are still matters outstanding as detailed below (delete as appropriate)		
Ref. No. (as for Assessment Form)	**Description**	**Can this be deferred to supervision?** *(If answering no the presumption will be that this is a reason to refuse the application, unless indicated otherwise)*
		…tab to extend table

Table 2: If differences of opinion between assessors have needed to be escalated for formal reconciliation, please provide details		
Ref. No.	**Detail**	**Outcome**
		…tab to extend table

Table 3: Follow-up of past supervision, applicant's accident/incident reports and results of past applicant's internal audit(s) (if any) *(Check whether all open points (if any) are closed since last assessment)*		
Document Ref.	**Detail**	**Comments**
		…tab to extend table

Table 4: Points for later supervision		
Detail	**Reason**	**Priority (High/medium/low)**
		…tab to extend table

Final recommendation			
The application has been properly assessed in line with the documented procedures		Yes ☐ No ☐	
I recommend that this application is		Accepted ☐ Refused ☐	
Give reasons for recommendation including details of key strengths and/or weaknesses, referring to table 1 as appropriate. …tab to extend table			
Assessor's Signature *(If several assessors, Lead Assessor has to sign the report)*		**Date**	

Part B: Accountable Manager's Recommendation	**Accountable Manager Initials**
I confirm that the applicant has/has not* complied with all relevant assessment criteria. (*delete as appropriate)	
I agree/disagree* with the assessor(s)'s conclusion regarding outstanding matters in relation to compliance with the criteria. Where disagreeing, give details of proposed alternative action. (*delete as appropriate)	

Part B: Accountable Manager's Recommendation			**Accountable Manager Initials**
I confirm that any differences of professional opinion with regard to this case have/have not* been resolved. Acceptance should therefore be escalated*. (*delete as appropriate)			
I recommend that a certificate* and/or authorisation* be issued/ I recommend the application be refused* (*delete as appropriate)			
In the case of a refusal recommendation			
I confirm that the applicant has been informed of the severity of outstanding matters of non-compliance and has been given all reasonable opportunity to respond. The actions set out below have been taken to secure this.			
Summary of Actions and their content			**Date of Action**
Accountable Manager's Signature		**Date**	

Part C: Assurance process	**Y/N/NA**
The **First Screen** and **Initial Review** have been carried out, and any requests for further information made to the applicant at this stage have been received;	
There is sufficient evidence to show that all relevant aspects of the application have been assessed by at least one assessor;	
Where areas of non-compliance with the assessment criteria have been identified, details have been provided; *(the accountable manager should **NOT** examine the details themselves as this will constitute revisiting the assessment)*	
The reports adequately reflect all findings of assessor(s);	
The **Assessment Form (Part 1)** has been sent to the applicant, and the applicant has been given sufficient opportunity to respond to matters raised;	
Where a meeting was held with the applicant, an adequate record of this is held;	
Written responses to all matters of non-compliance and requests for further information have been received from the applicant;	
Issues of non-compliance were all resolved in some way **or** where not resolved the assessor's reasons for this were clearly documented;	

Part C: Assurance process		**Y/N/NA**	
The Assessor(s) and Accountable Manager's recommendations given on the Assessment Report reflect the assessment as a whole;			
I confirm that the application has been properly assessed in line with the documented procedures.			
Any other comments: …press return to extend			
Assuror's **Signature**		**Date**	