

# Chapter 14

## Independent Professional Review

ESM activities you carry out must be reviewed by professionals who are not involved in the activities concerned.

### 14.1 Guidance from volume 1

These reviews are normally structured as a series of safety audits and safety assessments. They assure that the work has been carried out safely and provide evidence to support the safety case. How often and how thoroughly each type of review is carried out, and the degree of independence of the reviewer, will depend on the project. They will depend on the amount of risk and novelty and on how complicated the project is.

### 14.2 Background

Review of safety-related projects by professionals independent of the work is an important contribution to the confidence in the safety of the change being made to the railway.

We divide independent professional review into two activities:

- Safety Audits focus on the ESM processes being used and check that they are adequate and are being followed.
- Safety Assessments focus on the product of the project and check that the risk associated with the system being developed is (or will be) reduced to an adequate level.

In practice there is overlap between the two.

There is variation in terminology and practice in this area. Some practitioners divide the topic of independent professional review up differently and use the phrases 'Safety Audit' and 'Safety Assessment' with different meanings. For example, a distinction is sometimes drawn between technical assessment of engineering design and process assessment of safety management activities. You may need to refer to the guidance under both the audit and assessment headings even if the activity that you are asked to commission or perform is described as one or the other type of review.

This chapter describes these two types of review and the documentation that is required by them. It also discusses how to go about commissioning a review, what the reviews should be checking for, and how the results should be used. Outlines and checklists are provided in appendices B and C, respectively.

This chapter is written for Project Managers who will need to commission reviews and interpret the results, and the auditors and assessors who will be performing them.

## **14.3 Safety Audits and Assessments**

### **14.3.1 Safety Audits**

Safety Audits are intended to check that the ESM of a project is adequate and has been carried out in conformance with the Safety Plan. If there is no Safety Plan, one should be written before a Safety Audit is carried out.

The primary output of an audit is a Safety Audit Report. This report should include: a judgement on the extent of the project's compliance with the Safety Plan; a judgement on the adequacy of the Safety Plan; and recommendations for action to comply with the Plan or to improve it.

A Safety Audit should consider:

- work since the previous audit (all work so far if first audit);
- plans for the next stage;
- recommendations of the previous audit.

### **14.3.2 Safety Assessments**

Safety Assessment is the process of forming a judgement as to whether or not the risk associated with the system being developed is (or will be) reduced to an adequate level.

The safety requirements for the system are central to a Safety Assessment. The assessor should review the Safety Requirements Specification to assess whether it is sufficient to control risk and review the system to assess whether or not it meets or will meet the Safety Requirements Specification.

Safety Assessment involves the use of design analysis, auditing techniques and practical assessment by competent and experienced persons.

The assessor should also review the processes and organisation employed on the project. This aspect of the assessment is easier if the results of a recent Safety Audit are available. If a Safety Audit has not been carried out on the project recently enough that its conclusions are still valid, then one should be commissioned before a Safety Assessment, to ensure that the documentation to be assessed has been produced under a correctly applied Safety Plan. If the audit results are unsatisfactory then the assessment may be postponed until corrective action has been taken.

The result of a Safety Assessment is a Safety Assessment Report. This report should include an assessment on whether or not the risk associated with the system being developed is (or will be) reduced to an adequate level and recommendations for corrective action if necessary.

If the risk is not assessed as acceptable then the system may need to be re-assessed after corrective action is taken.

## **14.4 Commissioning a Safety Audit or Assessment**

In general the frequency and depth of each type of review and the level of independence of the reviewer (the Safety Auditor or Safety Assessor) will depend on the complexity and level of risk presented by the project.

Typically, Safety Audits and Assessments of the simplest and lowest risk projects should not take more than about a day of effort from a single auditor or assessor. Safety Audits of the most complex and highest risk projects may involve much more effort from an independent organisation.

Audits and assessments should be commissioned at the points defined in the Safety Plan (see chapter 12). The Project Manager or Safety Authority may commission additional audits or assessments.

Whoever commissions an audit or assessment should write a Safety Audit/Assessment Remit. This should record the requirements of the Audit or Assessment and all the relevant details, including:

- 1 the project title and reference;
- 2 the name of the Safety Auditor/Assessor, their qualifications and experience, and their level of independence;
- 3 references to previous audits and assessments;
- 4 audit or assessment requirements defining:
  - a) the scope of the audit/assessment which may be limited in extent (for instance, to a part of the system) or in time (for instance, to changes since the last release);
  - b) the purpose of the audit/assessment (for instance, to support a submission for safety approval);
  - c) the basis of the audit/assessment. For an audit this will define the documents that the project will be audited against (normally the Safety Plan and the documents that it references). For an assessment this should specify the legal framework (for instance, the ALARP principle in the UK) and the ESM framework (for instance, the Yellow Book) within which the project is being run; and
  - d) any previous assessments or audits whose results may be assumed in the performance of the current audit/assessment.

The remit should be agreed and signed by the Project Manager and the Safety Auditor/Assessor. An outline for a Safety Audit/Assessment remit is provided in appendix B and an example generic Safety Assessment remit is provided in appendix D.

#### 14.4.1 Independence

The Safety Auditor/Assessor should be independent of the project. Whoever commissions an audit or assessment should decide the level of independence. The following paragraphs provide guidance only.

The level of independence should be dependent primarily on the level of risk presented by the project (for electronic systems this is indicated by the Safety Integrity Level (SIL) of the system or equipment being developed. SILs are discussed in chapter 9.)

Table 14-1 provides guidance (derived from IEC 61508 [F.14]) on the level of independence appropriate at each SIL. Note that 'HR' indicates Highly Recommended, 'NR' indicates Not Recommended, and '-' indicates no recommendation for or against; however, a lower level of independence may be chosen by agreement with the Safety Authority. For the highest risk projects the Safety Auditor or Assessor should work for an independent organisation. For the lowest risk projects they may be organisationally close to the project, but should not be working on the project.

MINIMUM LEVEL OF INDEPENDENCE	SAFETY INTEGRITY LEVEL			
	1	2	3	4
Independent Person	HR	HR	NR	NR
Independent Department	-	HR	HR	NR
Independent Organisation	-	-	HR	HR

**Table 14-1 - Levels of independence at each SIL**

Where the Safety Integrity Level of the system or equipment is not known, for example when Safety Requirements have not yet been set, the level of independence should depend on the likely consequence of an accident caused by the system or equipment. Table 14-2 provides guidance on the level of independence appropriate at each classification of consequence defined in chapter 8. The nomenclature is as for Table 14-1.

MINIMUM LEVEL OF INDEPENDENCE	CONSEQUENCE			
	Negligible	Marginal	Critical	Catastrophic
Independent Person	HR	HR	NR	NR
Independent Department	-	HR	HR	-
Independent Organisation	-	-	HR	HR

**Table 14-2 - Levels of independence at each consequence category**

Where the tables indicate a choice of independence (for example, Table 14-1 indicates that both Independent Person and Independent Department are Highly Recommended for a SIL 2 system), the following factors should be considered in deciding an appropriate level of independence:

- the degree of previous experience with a similar design;
- the degree of complexity;
- the degree of novelty of the design, or technology; and
- the degree of standardisation of design features.

These factors may also guide the determination of the duration of a particular Safety Audit or Assessment. For example a system development utilising a novel technology is likely to require a more extensive Safety Audit/Assessment than a development using proven technology.

#### 14.4.2 Qualifications

The Safety Auditor should have the following qualifications:

- prior experience as a Safety Auditor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment;
- experience of process assurance (for instance quality or safety audits);
- familiarity with external safety standards and procedures;

- familiarity with the legal and safety regulatory framework within which UK railways operate;
- training in ESM.

The Safety Assessor should have the following qualifications:

- Chartered Engineer status in an engineering or scientific discipline relevant to the system or equipment;
- prior experience as a Safety Assessor or safety engineer for a minimum of 5 years in areas relevant to the system or equipment;
- demonstrable application domain experience;
- experience of process assurance (for instance quality or safety audits);
- familiarity with external safety standards and procedures;
- familiarity with the legal and safety regulatory framework within which UK railways operate;
- training in ESM.

The following factors should be taken into account in establishing the relevance of experience:

- purpose of the project;
- technology and methods used;
- Safety Integrity Level and accident potential.

Where a Safety Assessment is carried out by a team, the team as a whole should exhibit the necessary domain and process assurance experience and the lead assessor as an individual should possess the other qualifications.

It is a good idea to retain the same Safety Auditor and Assessor throughout the project.

#### 14.4.3 Depth of review

Engineering judgement should be applied to determine the degree to which the guidance above need be applied on a particular project. For the simplest and lowest risk projects, for example:

- The requirements for Safety Auditor or Assessor qualifications may be relaxed.
- Audit or Assessment activities listed in section 14.5 may be limited to interviewing personnel and reviewing documentation.
- The detail of the audit checklist or assessment checklist may be reduced.
- The Safety Audit or Assessment Report described in appendix B should concentrate on the findings and recommendations of the Safety Audit; the requirements and audit details sections should be brief.

The Safety Audit or Assessment Report should record and justify significant changes to the processes defined in section 14.5.

The Safety Assessment Report should concentrate on the findings and recommendations of the Safety Assessment; the requirements and assessment details sections should be brief.

#### 14.4.4 Roles and responsibilities

The Project Manager is responsible for:

- initiating Safety Audits or Assessments when scheduled in the Safety Plan;
- preparing the Safety Audit/Assessment requirements;
- appointing an auditor or assessor acceptable to the Safety Authority;
- ensuring the auditor/assessor has appropriate access to personnel, the Hazard Log and other documents;
- commenting on the Safety Audit or Assessment Report;
- formulating any necessary improvement actions in response to the report's recommendations;
- passing on any parts of the report which materially affect the Safety Assessment process to the Safety Authority; and
- implementing the improvement actions.

The Safety Auditor is responsible for:

- planning the Safety Audit;
- carrying out the Safety Audit; and
- preparing a Safety Audit Report.

The Safety Assessor is responsible for:

- planning the Safety Assessment;
- carrying out the Safety Assessment; and
- preparing a Safety Assessment Report.

### 14.5 The Safety Audit and Assessment processes

#### 14.5.1 Performing a Safety Audit

The Safety Audit process consists of three activities:

- 1 Planning the Safety Audit and producing an audit schedule;
- 2 Executing the audit schedule;
- 3 Preparing the Safety Audit Report.

The audit schedule should be produced by the Safety Auditor and endorsed by the Project Manager. Planned activities may be modified to reflect any required change of emphasis based on information gathered during the audit, although it is not always necessary for the audit schedule to be re-issued.

The schedule should be brief and should include:

- A statement of the audit requirements, according to the Audit Remit, but taking into account any agreed amendments;
- Identification of audit activities to be undertaken;
- Identification of individuals to be interviewed;
- Identification of documentation to be examined;

- Audit time-scales;
- Safety Audit Report distribution and the expected date of issue.

During audit planning the Safety Auditor should become familiar with:

- The Safety Plan;
- The findings and recommendations of any previous Safety Audits;
- Details of progress since the last Safety Audit (if any);
- Details of the next stage of work;
- Details of project staffing.

This familiarisation should be achieved through a briefing with the Project Manager, and preliminary inspection of project documents.

The audit activities should include:

- Interviews with project personnel;
- Examination of project documents;
- Observation of normal working practices, project activities and conditions;
- Demonstrations arranged at the auditor's request.

The evidence for compliance or non-compliance with the Safety Plan that arises from these activities should be noted for inclusion in the Safety Audit Report.

#### 14.5.2 What to look for in a Safety Audit

The Safety Audit is a check for adequacy of the Safety Plan and compliance against the Safety Plan. The audit should check therefore, that the planned project activities are being or have been carried out and in the manner and to the standards prescribed in the Safety Plan.

The Safety Auditor should derive an audit checklist for the investigation, to guide the enquiries and to record results and evidence. An outline for the checklist and an example are included in appendix D. The format of the checklist should mirror that of the Safety Plan and associated ESM activities such that each aspect of these is directly addressed by a question in the checklist. It should be in the form of a checklist with questions that may be answered 'Yes' or 'No'.

The checklist should be drawn up to meet the audit requirements, using the documents referenced in the Remit. The auditor should note anything that he or she finds that is objectively wrong, whether or not it relates to a checklist item. Note that the checklist is an aid for the Safety Auditor – it should not be completed by the project personnel.

The audit should check that any standards or procedures called up by the Safety Plan have been correctly applied. It should also check that there is traceability from the Safety Plan to project activities that implement it.

The audit should look for documentary evidence that every safety activity has been carried out. The answer to each question on the audit checklist should be supported by documentary evidence.

All instances where there is no evidence of compliance should be documented in the Safety Audit Report along with a recommendation for remedial action. Each non-compliance should be identified in terms of the specific requirements of the Safety Plan. The auditor should classify each finding. A suggested classification is shown in section 14.6.

Audit findings should be documented on the checklist. Where evidence of compliance is lacking, further in-depth examination should be carried out.

Information gathered through interviews should, where possible, be verified by acquiring the same information from other independent sources.

### 14.5.3 Performing a Safety Assessment

The Safety Assessor should become familiar with:

- The Hazard Log;
- The Safety Plan;
- The Safety Requirements Specification;
- The findings and recommendations of any previous Safety Assessments or Safety Audits;
- Details of progress since the last Safety Assessment;
- Details of the next stage of work.

This familiarisation should be achieved through a briefing with the Project Manager, and preliminary inspection of project documents.

The Safety Assessor should prepare an assessment plan. The plan should be brief and should include:

- A statement of the assessment requirements, according to the assessment remit, but taking into account any agreed amendments;
- Identification of any dependencies on the project or others, such as access to project personnel or documents;
- Identification of the assessor or assessment team, including qualifications, experience and level of independence;
- Identification of individuals to be interviewed;
- Management arrangements for reporting findings and reviewing, endorsing and distributing the Safety Assessment Report;
- Assessment time-scales, including the expected date of issue of the Safety Assessment Report.

The assessment activities should include:

- Interviews with project personnel;
- Examination of project documents;
- Observation of normal working practices, project activities and conditions;
- Re-work of parts of the safety analysis work to check accuracy, concentrating on particularly critical areas or where the assessor has reason to suspect a problem;
- Demonstrations arranged at the assessor's request.

#### 14.5.4 What to look for in a Safety Assessment

The primary objective in planning and carrying out a Safety Assessment is to make sure that you collect enough information to support a judgement on the acceptability of the risk. The following guidance may help in planning the assessment but you should also employ your professional judgement and experience to tailor the guidance to the application in hand.

The assessment should examine the development or application process, review the design decisions taken by the project staff which have safety implications and verify that that risk has been reduced As Low As Reasonably Practicable (ALARP) and in accordance with the Safety Requirements.

The Safety Assessor should derive an assessment checklist to guide the enquiries and to record results and evidence. Example checklists are presented in appendix D. The checklist should be drawn up to meet the assessment requirements, using the documents referenced in the remit. The assessor should note anything that he or she finds that is objectively wrong, whether or not it relates to a checklist item. Note that these checklists are an aid for the Safety Assessor – they should not be completed by the project personnel.

The assessment should not just focus on documents but should look at the processes and organisation behind them. The assessor should look for any shortcomings in the approach to safety and make recommendations.

The assessment should pay particular attention to the Hazard Log, which should provide traceability from the Safety Requirements to documentation supporting engineering activities on the project.

The assessment should check that there is documentary evidence for every safety activity carried out. The answer to each question on the assessment checklist should be supported by documentary evidence.

If operational data is available, the assessor should analyse it for evidence of:

- hazards not previously identified;
- risks incorrectly classified;
- Safety Requirements not met;
- changes in the pattern of operational use.

The Safety Assessor may call for the repetition of any formal tests and the Project Manager should arrange for these to be run under the Safety Assessor's supervision.

If a previous assessment has been carried out and has not been invalidated by changes to the design or new knowledge then the assessor need not repeat the analyses carried out there and should concentrate instead on analysing new and changed material.

If the assessment detects a flaw in the ESM programme then the assessor should review the ESM documentation to establish the most likely root cause. The assessor should consider whether this throws doubt on any other aspects of the ESM, and the assessment recommendations should include measures to restore confidence in affected areas as well as addressing the defects detected.

Information gathered through interviews should, where possible, be verified by checking the same information from other independent sources.

### 14.5.5 Findings

Findings should be communicated to the Project Manager and project team as soon as possible. You should not wait until the Safety Audit/Assessment Report is prepared and distributed.

This may conveniently be done with a simple three-part form:

- Part 1: Finding
- Part 2: Project response
- Part 3: Assessor's/auditor's comments on project response.

### 14.6 Audit/assessment findings

All auditor's and assessor's findings should be uniquely numbered and classified. The following classification scheme is widely used and is recommended. Categories 1 to 3 should be used when the audit/assessment is supporting a request for safety approval.

**Category 1** - Issue is sufficiently important to require (substantial) resolution, prior to recommending that the change may become operational. (Alternatively a specific control measure may be implemented to control the risk in the short term.)

**Category 2** - Issue is sufficiently important to require resolution within 3-6 months, but the change may become operational in the interim (possibly with a protective control measure.)

**Category 3** - Issue is highlighted for incorporation into the Safety Case at the next periodic review, but no action is required separately.

Where there are a large number of lower category issues, the auditor/assessor should consider whether, in totality, they represent sufficient residual risk that they in effect equate to one or more higher category issues (that is, that they would warrant the imposition of any additional mitigating control measures). In these circumstances, it should be considered whether these outstanding issues relate to an overall lack of rigour or quality in the document that has been reviewed.

The Project Manager should review and endorse the Safety Audit/Assessment Report, and formulate improvement actions in response to the Safety Auditor's/Assessor's findings. It may be appropriate to record any faults discovered in the system itself in the Data Recording and Corrective Actions System (see chapter 12). The Project Manager should implement these improvement actions.

The Safety Assessment Report may include recommendations for action by the relevant Safety Authorities, for example reviewing the approval of systems or equipment in service. If the report contains any such recommendations the Project Manager should pass that part of the report to the relevant Safety Authorities, who should then consider any such recommendations and implement promptly any necessary actions.

**14.7 Related guidance**

Chapter 8 provides guidance on risk assessment

Chapter 9 provides guidance on the safety requirements specification and Safety Integrity Levels.

Chapter 12 provides guidance on safety planning.

Appendix B provides outline audit and assessment remits and reports.

Appendix D provides an example assessment remit and example audit and assessment checklists.

This page left intentionally blank