ISAs – Saving for the Future

J.R. Inge, MEng PGDip(SCSE) CEng MIET MAPM; Ministry of Defence; Bristol, UK

Keywords: ISA, independent safety audit, assurance, competence, code of practice

Abstract

Independent Safety Audit features in many Ministry of Defence policies, but its role is often not well understood. This paper examines the various different MOD policy requirements for independent safety audit and looks at how those requirements can be fulfilled. It attempts to demystify the process of contracting for ISA work by introducing sources of guidance for project staff, including the recently developed Code of Practice and Competence Framework developed by the IET/BCS Independent Safety Assurance Working Group. The paper also briefly examines what impact the recent report of Charles Haddon-Cave QC into the loss of Nimrod XV230 is likely to have on the role of Independent Safety Audit.

Introduction

In the UK Ministry of Defence (MOD), the role of an Independent Safety Auditor (ISA) is to act as the professional conscience of a Duty Holder[1]. According to Defence Standard (Def Stan) 00-56, an ISA is "*An individual or team, from an independent organisation, that undertakes audits and other assessment activities to provide assurance that safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose.*" [1] The ISA does not make executive decisions about the safety of the system in question, but acts in an advisory capacity, giving the Duty Holder confidence in the evidence with which they are presented.

The acronym 'ISA' is often used to refer to other activities beyond Independent Safety Audit, with the 'A' variously expanding to mean 'assuror', 'assessor', 'accreditor', or 'advisor'. These can all be valid roles in a project or other safety-related undertaking and are often used to refer to activities with overlapping scope. The joint Independent Safety Assurance Working Group of the Institution of Engineering & Technology and the British Computer Society has used the generic term 'Assurance' to cover the general requirement, and 'Assessor' to refer to the individual role [2]. In general, the ISA role is one of assurance: the customer seeks to gain assurance that the safety effort is adequate. Safety audits and accreditation against standards are two tools that might contribute to providing this assurance. Precisely which terminology is used depends on the domain, with different industries using different terms.

For instance, the railway industry's Yellow Book recommends Independent Professional Review, with one of its Engineering Safety Management fundamentals being that "*Safety management activities … must be reviewed by professionals who are not involved in the activities concerned*." The guidance on these reviews refers to Independent Safety Audits and Assessments. In this context, Independent Safety Audits check that safety management plans are being followed, while Independent Safety Assessments check that safety requirements are (or will be) met [3]. Similar distinctions are also made in other domains.

A particularly important distinction to understand is that between an Independent Safety Auditor and an Independent Safety Advisor. An Independent Safety Auditor does provide advice, in the sense that they advise the Duty Holder on the adequacy of the safety case and safety arrangements in general. They might also point out weak points in the system or the management arrangements, and give the sort of generic advice found in official guidance documents, standards or codes of practice. However, the amount of advice that they can give on how to design the system or set up the specific arrangements is limited: once they start to influence the design, they have lost their independence. It would be entirely appropriate for a Duty Holder to employ someone from an independent organisation to provide such design advice, to increase the competence of the project team, but such a person could not also perform the role of Independent Safety Auditor.

[1] Duty Holder: the person with specific responsibility for the safety management of a system.

The ISA Requirement

What are we trying to achieve?

Independent Safety Audit forms a part of the MOD's safety management system, and as such, is primarily aimed at avoiding preventable accidents. While safety audit is generally applicable to all sorts of safety-related activity, Def Stan 00-56 envisages a customer-supplier scenario, where the customer is normally a MOD project team and the supplier is a prime defence contractor. The project team must help fulfil the MOD's responsibility to supply safe equipment and working environments to its staff, while the contractor must fulfil their responsibility to supply equipment or services that are safe for use. However, this is a business environment and there are pressures on both sides which are not necessarily in the interests of safety: projects must be delivered within a time, cost and performance envelope. Equally, when projects are delivered by dedicated MOD or industry teams, there is the possibility that familiarity with the work can allow safety hazards to become overlooked. In this context, "*The objective of independent assessment is to overcome possible conflicts of interest and oversights that may arise from the use of a single organisation*". [4]

Beyond the safety objective, independent safety audit also forms part of the governance and management of projects. While we are interested in ensuring that defence capability is safe, we are also interested in delivering it effectively: on-time and on-budget, with the required performance. The role of independent safety audit here is to help with early identification of safety issues that might cause risks to the project. If a safety issue is identified in a system, it is much cheaper and easier to make alterations early in the project, rather than waiting until after the design has been frozen, or the system manufactured. When problems are identified late, it can lead to delays in deployment, costly modifications, or avoidable limitations on capability. Early identification of safety issues also means that they can be resolved more effectively, through technical measures rather than procedural limitations. The hope is that by investing in Independent Safety Audit from the early stage of a project, the MOD will make future savings in terms of reduced project delivery costs and a lower level of accidents when systems are deployed.

Def Stan 00-56

Although Def Stan 00-56 is the source of the MOD's definition of the role of an Independent Safety Auditor, the current issue does not in fact require an ISA to be appointed or give any requirements for their scope of work. Instead, it provides a contractual vehicle for ensuring that if the customer does appoint an ISA, the ISA will have the access they need to a contractor's records and premises, in order to carry out their work.

Def Stan 00-56 allows the ISA to be appointed either by the Duty Holder or by the contractor. It is normally recommended that the ISA is customer-appointed, to help ensure commercial independence from the contractor, and this is the default position in the standard. However in some cases it may be preferable for a contractor to appoint the ISA themselves, e.g. where a prime contractor is also a Duty Holder, or is acting as a system integrator and taking on more of the traditional customer project management roles.

In return for giving access to the project, Def Stan 00-56 gives the contractor rights to protect their commercial interests, through confidentiality agreements and the ability to reject ISAs employed by competitors. Similarly, it gives the Duty Holder the right to reject the contractor's choice of ISA. [1]

Def Stan 00-56 does not insist that an ISA be appointed, because whether an ISA is necessary or not varies according to the circumstances of the project. Project teams should look to the relevant functional safety policy document for their domain, to find out what is appropriate. Normally this is specified in one of Joint Service Publications covering functional safety in a particular domain.

Requirements on MOD staff

Joint Service Publications (JSPs) are the MOD's high-level internal policy documents. Each JSP generally covers a specific domain, technology or type of activity, but applies across all business units of the MOD. For safety, the top-level JSP is JSP 815 – *Defence Environment and Safety Management*, which sets out a policy framework. Beneath JSP 815 are a number of "Level 2" JSPs that set domain-specific requirements for management of functional safety in the land, sea and air domains, and for specific technologies such as ordnance, nuclear or fuels and gases. It is these policy documents that set out what MOD staff are required to achieve through Independent Safety Audit.

For maritime projects JSP 430 – *Ship Safety Management*, requires that an ISA is commissioned to undertake an independent review to confirm that the safety regime has been implemented in accordance with the policy and

that outputs of the regime, including the safety case, are comprehensive. The ISA is expected to endorse the safety case report. However, the requirement for an ISA may be waived for projects that are of sufficiently low complexity or risk. [5]

In the Land domain, JSP 454 – *Land Systems Safety and Environmental Protection*, uses very similar wording to JSP 430, but the bias is changed. JSP 454 does not mandate that projects should always use an ISA, but does recommend it for projects with significant risk or complexity. [6]

Under JSP 553, the *Military Airworthiness Regulations*, project team leaders are required to ensure that Designers' safety cases are independently assessed. The requirement is broken down into two elements: Independent Safety Audit (process audit against the safety plan) and Independent Technical Evaluation (technical analysis of the safety case evidence). The requirement is obligatory for systems in higher risk classes and desirable in other cases where novel, complex, or high-risk systems are involved. JSP 553 also recognises that Independent Safety Audit should support the in-service safety case, requiring the Release To Service Authority to ensure that the level of required independent safety audit and evaluation of the safety case is identified and applied, and an Independent Safety Auditor appointed where appropriate.

JSP 518 – *Regulation of the Naval Nuclear Propulsion Programme* does not mention Independent Safety Audit as such, although it contains similar concepts. Independent Nuclear Safety Assessment provides an independent assessment of the adequacy of the Safety Justification documentation with regard to its basis, completeness and whether it demonstrates that the risk presented is acceptable. This is carried out by a separate organisation to that making the safety justification. Independent Peer Review is also used, to examine documentation to consider its acceptability and completeness. This will be commissioned by the organisation making the justification, but use independent resource [7].

Requirements on ISAs

The Joint Service Publications are written to apply to MOD staff, and as such do not apply directly to contractors. Instead, the MOD must place contractual requirements onto its suppliers that ensure that relevant aspects of the JSPs will be fulfilled. Def Stan 00-56 gives a standard, contractual way of asking a prime contractor to work with an ISA, but it does not mandate what the ISA should actually do. There is not an equivalent standard for tasking an ISA, and project teams need to decide this for themselves.

Luckily, guidance for the selection of an ISA and the preparation of their tasking is available from various sources, including the Project Oriented Safety Management System (POSMS), the Acquisition Operating Framework, the IET/BCS Independent Safety Assurance Working Group, and the JSPs themselves.

Guidance for procuring ISA services

Tasking an ISA

The functional safety JSPs allow varying amounts of discretion in whether an ISA is required for a given project, and what they are tasked to do. The factors affecting this decision include the potential risk involved (i.e. the risk before mitigation), the degree of complexity and novelty of the undertaking.

It is sensible to conduct a preliminary hazard identification exercise as early as possible in a project, to identify the general type and level of risks that might be expected. This can often be done at a functional or capability level, before any of the actual system design is known. This analysis can then inform judgements about the level of assurance that will be required for the project. Where the system is particularly complex, or involves novel technologies or solutions, there will be greater uncertainty and more assurance is likely to be required. If however it is decided not to appoint an ISA (and the relevant JSP permits it), then that decision should be recorded and justified.

Having decided that an ISA is to be appointed, their terms of reference need to be determined and recorded. The guidance part of Def Stan 00-56 recommends that the ISA should be part of the project safety committee, and that their report should be part of (or referenced in) the safety case report [8]. The ISA would normally be expected to provide endorsement of safety case reports, and the Defence Equipment & Support's Project Oriented Safety Management System (POSMS) also suggests that they should endorse hazard identification and risk estimation work. The Def Stan 00-56 definition of ISA breaks down into three main activities:

- Providing assurance that safety activities comply with planned arrangements (through undertaking audits and other assessment activities);

- Providing assurance that safety activities are implemented effectively and are suitable to achieve objectives; and

- Providing assurance that related outputs are correct, valid and fit for purpose.

The scope of an ISA's tasking across these activities may be affected by the regulatory environment and the structure of the project's organisation. The MOD will need to gather safety assurance about the whole capability it provides to front line users. Some parts of the capability may be provided by one or more defence contractors (by supplying equipment or services), while others may be provided by different parts of the MOD. The MOD Duty Holder will need to consider how assurance is gained about each of these parts, and about how the parts are integrated together. It may therefore be appropriate to task the ISA to investigate aspects of the MOD's business, as well as that of contractors.

In a similar vein, some parts of a project may receive independent scrutiny through other means, e.g. the Key Hazard Certification process in the maritime domain. Projects should therefore consider how they get assurance about the adequacy of the totality of the safety evidence: which parts should be assessed by an ISA, and which by other independent agencies.

Detailed advice on setting terms of reference for ISAs can be found in the document *Guidance for Integrated Project Teams for Use in Contracting for Independent Safety Auditor (ISA) Services* [9]. This is available through the Acquisition Operating Framework[2] (search for 'ISA') or from the ISA Working Group's web pages. Although dating from 2004, a recent study has found that it is still relevant to current requirements [10]. The guide considers the selection of an ISA, their interface with other parts of the safety regime, and the different scopes of work that might be appropriate at different stages of the life cycle of a project.

Selecting an ISA

Selection and appointment of an ISA should take place as early as possible in the project life, to allow key safety decisions to be influenced [8]. The key factors affecting the decision of which ISA to select will be the level of competence and the level of independence required. Both these factors are a matter of judgement and need to be tailored to the project.

An ISA's competence will be made up from a combination of qualifications or accreditations, experience and knowledge. Some of this competence will be generic, relating to auditing and to common safety management tools and techniques. However, an ISA will also require specialist knowledge of the project's problem domain and the technologies being used. For some simple projects this competence may be vested in a single individual, but for other more complex undertakings this means that the ISA may need to be a competent team. Equally, if the scope of the project changes significantly, it may mean that the competence requirements for the ISA will also change.

The level of independence required of an ISA will vary according to the risk and complexity of the project, in a similar manner to the level of scrutiny required. For simple, low-risk pieces of work, it may be appropriate to use someone from the same organisation, who is not directly involved in the work. As the risk increases, it would be more appropriate to use someone from a different department, or a totally different organisation. The ISA should be able to demonstrate financial and commercial independence from the project, and should not have a vested interest in its outcome. This means that it is normally more appropriate for an ISA to be contracted by the MOD directly, rather than via a prime contractor.

Many ISAs are available to be tasked through the MOD's Framework Agreement for Technical Services (FATS)[3]. This is a commercial arrangement with preset rates that allows work to be tasked quickly without drawing up a full new contract, and with only limited competition. Where FATS is not appropriate (e.g. when the required competence is not available through the FATS Market Knowledge Matrix), an ISA would need to be contracted directly.

Further guidance on how to select an ISA may be found in the Guide mentioned in the previous section, and also in two new tools recently developed by the IET/BCS Independent Safety Assurance Working Group. The group has recently published a Code of Practice for ISAs [11] and a Competency Framework for ISAs [12], which are discussed in the next section.

---

[2] www.aof.mod.uk

[3] www.mod.uk/DefenceInternet/FactSheets/TheFrameworkAgreementforTechnicalSupportfats.htm

Code of Practice for ISAs

The ISA WG Code of Practice [11] aims to provide clarity in how the ISA role is carried out. It is recognised that the ISA role crosses many different disciplines and does not fall squarely into the remit of a particular professional institution. Thus it builds on the codes of existing professional bodies, concisely covering just those issues that are particular to ISA work.

The code is targeted both at ISAs themselves, to allow them to demonstrate their commitment to professionalism; and at their customers, to guide their expectations. As industry good practice, project teams would be recommended to choose ISAs who follow the code. Teams can use the code when drawing up selection criteria and assessing tenders for ISA work.

The body of the code defines ten requirements for professionals carrying out independent safety assessments. These requirements cover general professional conduct, independence, competence, communication, proportionality, advice, integrity, priority of safety, escalation, and management & planning. Each requirement is a simple statement, supported by bullet points giving further advice and interpretation. The Code is freely available from the ISA Working Group's web page[4].

Competence Framework for ISAs

One of the requirements of the Code of Practice for ISAs is that "the ISA should be demonstrably competent to undertake the assessment activities, to make judgements regarding safety, and to communicate effectively the results of their work". Similar requirements are found in various MOD policy and guidance documents. However, it is not immediately clear what these competence requirements really are, or how they should be demonstrated.

As was mentioned above, the competence required to carry out an ISA task will vary to some extent from project to project, so hard and fast generic requirements cannot be set. Instead, the ISA Working Group has devised a competence framework that can be used as a prompt to set specific competence requirements for a particular task, or to help an organisation that provides ISA services to put in place their own competence management system.

The Competence Framework for ISAs [12] builds on the MOD's ISA Guidance document [9], the HSE's Blue and Red Books (*Competence Criteria for Safety Related Practitioners* and *Managing Competence for Safety-related Systems*), and other industry standards. It considers competence in three main areas: technical competence, behavioural competence, and knowledge. Each of these is broken down into a number of sub-areas and examples of specific competences such as "performing HAZOPS" or "reporting and presentation skills". The list is not intended to be exhaustive, rather a guide to the type of areas that might need to be covered. In each case, there are pointers to more detailed sources of information, such as the HSE Blue Book. Levels of competence are defined using a scheme of 'Supervised Practitioner' / 'Practitioner' / 'Expert', as used in the Blue Book and the MOD's own System Safety competence set. A useful feature of the document is the guidance that it provides on how to procure ISA services, showing the types of information that the customer needs to provide alongside the tasking, and how the ISA should respond in order to justify their competence.

Haddon-Cave and the Future Role of ISAs

The most influential report of recent years concerning safety in the MOD is the Nimrod Review produced by Charles Haddon-Cave QC [13]. The review focuses on the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006, but is recognised as having wider applicability to other domains of the MOD.

A key line of argument in the report is that the ISA failed to give proper scrutiny to safety case documents before signing them off. As a result, the Nimrod was allowed to continue flying despite flaws in its design that ultimately led to a tragic loss of life. These flaws had been identified during the risk assessment process, but had not been adequately addressed. The failings in the ISA role were sufficiently important that Haddon-Cave felt it in the public interest to name and shame two of the individuals involved, and his report repeatedly emphasises the importance of independent assurance, calling it "*the 'third stool'* [sic] *in the safety process*".

[4] www.theiet.org/publicaffairs/panels/isa/

However, one of the failings that the report reveals is that the ISA role was never made clear. The ISA was employed as an 'Advisor', although there was an expectation that they would perform the role of an 'Auditor' as per Def Stan 00-56 and JSP 553. Unfortunately, no terms of reference or audit plan was drawn up and audits were not carried out. Furthermore, Haddon-Cave found that where safety case audits are carried out, they tended to focus on the process rather than the substance of the safety case.

In his recommendations, Haddon-Cave sets out a number of principles for different parts of the MOD's airworthiness regime. The key principles are "*Leadership, Independence, People (not just Process and Paper), and Simplicity*". The Independence principle is clarified as requiring "*thorough independence throughout the regulatory regime, in particular in the setting of safety and airworthiness policy, regulation, auditing and enforcement*". Six principles for safety cases are also given, namely that they should be "*Succinct, Home-grown, Accessible, Proportionate, Easy to understand and Document-lite*" (SHAPED).

Haddon-Cave also makes recommendations about the organisation of the airworthiness regime, including the establishment of an independent airworthiness regulator (the Military Aviation Authority), and clear assignment of operational Duty Holder responsibilities to the Front-Line Command at corporate, operational and delivery level.

Taken together, Haddon-Cave's findings and recommendations imply that there will continue to be an important future role for Independent Safety Audit. However, the nature of that role may need to change in emphasis. The focus on the lead Duty Holder role of the operating authority has prompted a renewed realisation that safety cases need to consider all the Defence Lines of Development[5], rather than just the equipment and logistic aspects. They will also need to consider the interfaces with other systems and the wider MOD contribution to safety, rather than just constraining themselves to the scope of an equipment contract. As operating authorities start to take greater ownership of the overall safety case for their activities, more ISAs may be tasked directly by the front-line command headquarters, rather than by project teams in the Defence Equipment & Support organisation.

The call for safety cases to be Home-grown may result in more assurance work being done in-house in the MOD, perhaps through greater use of internal audit and peer review or a greater role for regulatory systems. The SHAPED principles also point towards a need to gain more assurance of the fitness for purpose of safety case deliverables: that they are tailored to their audience, proportionate to the potential risk and effective in demonstrating how that risk is controlled. This is likely to lead to a renewed emphasis on verifying the adequacy of safety case evidence, rather than just the process that is used to put the safety case together.

Conclusions

Independent Safety Audit is a valuable tool that can help projects make savings both through avoiding project costs and by preventing accidents. In order for this to be most effective, an ISA should be tasked early on in a project. The ISA should be given clear terms of reference, tailored to the specific circumstances of the project, and they should be selected to be suitably competent and independent. The importance of getting this right has recently been reinforced by the Haddon-Cave report [13].

MOD requirements for what should be achieved through Independent Safety Audit are set out in the functional safety Joint Service Publications, but must be tailored and made specific to individual projects. Guidance for how this should be done is primarily available via the Acquisition Operating Framework, in the document *Guidance for Integrated Project Teams for Use in Contracting for Independent Safety Auditor (ISA) Services* [9]. Having decided on terms of reference for an ISA task, a suitable, competent team or individual must be selected to carry out the role. A new Code of Practice and a Competence Framework for ISAs have been made available by the IET/BCS Independent Safety Assurance Working Group to help simplify this process [11, 12].

[5] Training, Equipment, Personnel, Infrastructure, Doctrine, Organisation, Information and Logistics.

References

[1] Directorate of Standardization. Safety management requirements for defence systems - part 1: Requirements. Defence Standard 00-56, Ministry of Defence, Glasgow, UK, June 2007. Issue 4.

[2] IET/BCS ISA Working Group. Independent Safety Assurance (ISA) working group. website. http://www.theiet.org/publicaffairs/panels/isa/index.cfm retrieved 19 Apr 2010.

[3] *Engineering Safety Management (The Yellow Book) - Fundamentals and Guidance*, volume 1 & 2. Rail Safety and Standards Board, London, UK, 4th edition, 2007.

[4] MOD Aviation Regulatory Group. Military airworthiness regulations. Joint Service Publication 553, Ministry of Defence, Bristol, UK, November 2009. 1st edition, change 7.

[5] Ship Safety Management Office. Ship safety management - part 1: Policy. Joint Service Publication 430, Ministry of Defence, Bristol, UK, September 2006. Issue 3 amdt 2.

[6] Land Systems Safety Office. Land systems safety and environmental protection - part 1: Policy. Joint Service Publication 454, Ministry of Defence, Bristol, UK, June 2009. Issue 5.

[7] Defence Nuclear Safety Regulator. Regulation of the naval nuclear propulsion programme. Joint Service Publication 518, Ministry of Defence, Bristol, UK, December 2008. Issue 3.0.

[8] Directorate of Standardization. Safety management requirements for defence systems - part 2: Guidance on a means of complying with part 1. Defence Standard 00-56, Ministry of Defence, Glasgow, UK, June 2007. Issue 4.

[9] Adelard; Ship Safety Management Office. Guidance for Integrated Project Teams for use in contracting for Independent Safety Auditor (ISA) services. Technical Report STG/181/1/9/1, Ministry of Defence, Bristol, UK, June 2004.

[10] S Rhys David. Report on SIWG action A3 – ISAs. Technical Report SAS/2106/04 R01, Ministry of Defence, Bristol, UK, March 2009. Draft C.

[11] Independent Safety Assurance Working Group. Code of practice for Independent Safety Assessors (ISAs). Technical report, Institution of Engineering and Technology; British Computer Society, London, UK, May 2009. Version 2.

[12] Independent Safety Assurance Working Group. Competency framework for Independent Safety Assessors (ISAs). Technical report, Institution of Engineering and Technology; British Computer Society, London, UK, October 2009. Issue 1.

[13] Charles Haddon-Cave QC. The Nimrod Review: An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006. Technical Report HC 1025, The Stationary Office, London, UK, October 2009.

Biography

J. R. Inge, Head of the Ship Safety Management Office, Ministry of Defence, Sea Systems Group, Elm 1c #4134, MOD Abbey Wood, Bristol BS34 8JH, UK, telephone – +44 (0) 30 679 35143, facsimile – +44 (0) 117 913 5943, email – DESSESea-SSMO@mod.uk.

Mr Inge was lead editor for Issue 4 of Defence Standard 00-56 – Safety Management Requirements for Defence Systems. His experience is as a project manager and safety policy specialist in the UK Ministry of Defence. He is a Chartered Engineer and holds a MEng from Durham University and a postgraduate diploma in Safety Critical Systems Engineering from the University of York. He contributes to the IET/BCS Independent Safety Assurance Working Group and the IET's Technical Advisory Panel on Functional Safety.