Ministry of Defence

JSP 815 Volume 2

Element 4: Risk Assessments and Safety Cases

Contents

Amendment record

This element has been reviewed by the Directorate of Defence Safety (DDS) together with relevant subject matter experts and key Safety stakeholders. Any suggestions for amendments **should** be sent to COO-DDS-GroupMailbox@mod.gov.uk.

Version No	Date published	Text Affected	Authority
1.0	Dec 22	BETA version for consultation	Dir HS&EP
1.1	7 June 23	Final version of Volume 2	DDS

Terms and definitions

General safety terms and definitions are provided in the Master Terms and Definitions Glossary which can also be accessed via the GOV.UK page.

Must and should

Where this element says **must**, this means that the action is a compulsory requirement.

Where this element says **should**, this means that the action is not a compulsory requirement but is considered good practice to comply with the policy.

Scope

This policy applies to all those employed by Defence (military or civilian) as well as those working on behalf of Defence (for example, contractors). It applies to all Defence activities carried out in any location (UK or overseas).

Introduction

1. This element provides the direction that must be followed and the guidance and good practice that should be followed and will assist users to comply with the expectations for risk assessments and safety cases that are set out in Element 4 of the Volume 1 to JSP 815 (this JSP).

Purpose and expectations

2. This guidance supports Defence organisations with putting in place suitable and sufficient methods for identifying hazards and assessing risks as a basis of effective control of safety risk. It also supports the development of safety cases, and the process by which they are reviewed to verify that equipment and systems are being safely designed, assessed during manufacture, construction, procurement and used for their intended purpose in the correct operating environment.

Management and assessment of safety risks

Risk management

3. UK H&S legislation (primarily the Health and Safety at Work etc Act 1974 Regulation 2) places general duties (criminal law) of employers to their employees and "it shall be the duty of every employer to ensure, so far as is reasonably practicable [SFAIRP][1], the health, safety and welfare at work of all his employees". Where there is a breach of this duty, this is commonly referred to in tort law (civil law) as the "duty of care." The legislation requires employers to fulfil their 'duty of care' responsibilities by reducing risks to as low as is reasonably practicable (ALARP). In accordance with the Secretary of State's (SofS) Policy these requirements apply to all Defence activities.

4. Risk management in Defence must be conducted in accordance with JSP 892 (Risk Management). Defence organisations should be able to demonstrate how effective risk management is incorporated into their Safety Management System (SMS) and that a risk management framework is in place. The risk management framework is owned by the senior leader within the Defence organisation and it should include risk identification, assessment, mitigation, reporting and monitoring, and governance in order to drive continual improvement in safety performance and to meet the Defence safety vision of eliminating fatalities, enhancing capability and minimising injury.

5. The risk management framework should set out how safety risks are effectively managed within their organisation, by making sure:

a. suitable and sufficient risk assessments are conducted and they are proportionate to the Defence activity that is being undertaken;

b. appropriate procedures for safe systems of work or training are in place;

c. competency requirements are defined for specific roles; and

d. there is an appropriate elevation process with ownership and acceptance of risk through the chain of command, including reasonably foreseeable risks to life (RtL).

[1] Defence more commonly uses the term as low as reasonably practicable (ALARP). The HSE consider that the two phrases (SFAIRP and ALARP) essentially mean the same thing. The term ALARP is generally used more in risk management and therefore why it is used in this Element. The key words in both phrases are "reasonably practicable" and this permits the employer to weigh a risk against the trouble, time and money needed to control it.

Risk profile

6. The risk profile is the examination of the hazards faced by an organisation and informs all aspects of the organisation's approach to leading and managing its safety risks. A risk profile examines:

a. the nature and level of the hazards

b. the likelihood of harm occurring

c. the severity of the harm associated with each type of hazard

d. the effectiveness of control measures in place.

7. Defence organisations are to establish their own risk profile for assessing and managing their safety risks. The risk profile should be regularly reviewed by their leadership and should be closely aligned with activity planning processes aided by the use of tools such as a strengths, weaknesses, opportunities and threats (SWOT) analysis.

Risk assessment

8. A risk assessment is focussed on the hazards arising from a specific activity and considers the likelihood of an event happening, and the severity of any potential harm or damage. It is about identifying foreseeable risks in the workplace and making sure that suitable and proportionate control measures are in place to mitigate them. Risk assessments and their associated control measures must be regularly reviewed at a frequency proportionate to the risk.

9. Defence organisations must make sure that suitable and sufficient risk assessments are carried out in accordance with JSP 375 Volume 1, Chapter 8 (Safety Risk Assessment and Safe Systems of Work), which sets out the following five-step risk assessment process:

Step 1 – Identify the hazards.

Step 2 – Decide who might be harmed and how.

Step 3 – Evaluate the risks and identify suitable and sufficient control measures.

Step 4 – Record and implement findings.

Step 5 – Review the assessment and update, as necessary.

10. Defence organisations must have an effective process in place to communicate the safety risks and associated control measures to all stakeholders, in order to provide safe working practices. This should include TU safety representatives, and other workforce representatives.

Risk mitigation

Reducing risks to ALARP

11. H&S legislation requires that action is taken to reduce or "mitigate" the level of risk to ALARP. The application of managing risks to ALARP should be understood and demonstrated by those who will be held personally accountable for the activity. Making sure a risk has been reduced to ALARP is about balancing the risk (as a consequential outcome) against the relative cost (in terms of money, time and effort) needed to control the risk.

12. To demonstrate that a risk is ALARP, the person controlling the activity must be able to show that the cost of applying further mitigation is grossly disproportionate to the risk reduction achieved. Even when a risk is mitigated to ALARP there may still be a high residual risk remaining.

13. The suitable and sufficient arrangements necessary to reduce risks to ALARP may include the expression of the risk assessment as a safety case and the provision of equipment, infrastructure, trained personnel and procedures of an appropriately high calibre. It should also be necessary to apply appropriately high management attention to certain activities to maintain the arrangements and to be able to respond to changes (including organisational changes.

Risk tolerability

14. Duty Holders have a responsibility to make sure that all RtL from military activities that require enhanced safety management arrangements are mitigated to ALARP and tolerable. This is in addition to a Defence organisation's duty of care responsibilities to mitigate risk to ALARP and tolerable. The concept of tolerability considers whether high risk activities should be undertaken by assessing the level of risk and the tolerability boundary. The tolerability boundaries will change depending upon the operating circumstances, as identified by the lines A and B shown in Figure 1 below.

15. The principle of tolerability is that the risk of injury or fatality within a workforce or wider society can be tolerated. A tolerable risk is one that we are willing to accept in order to perform an activity or achieve an outcome if it has been evaluated and is being managed to a level that is ALARP.

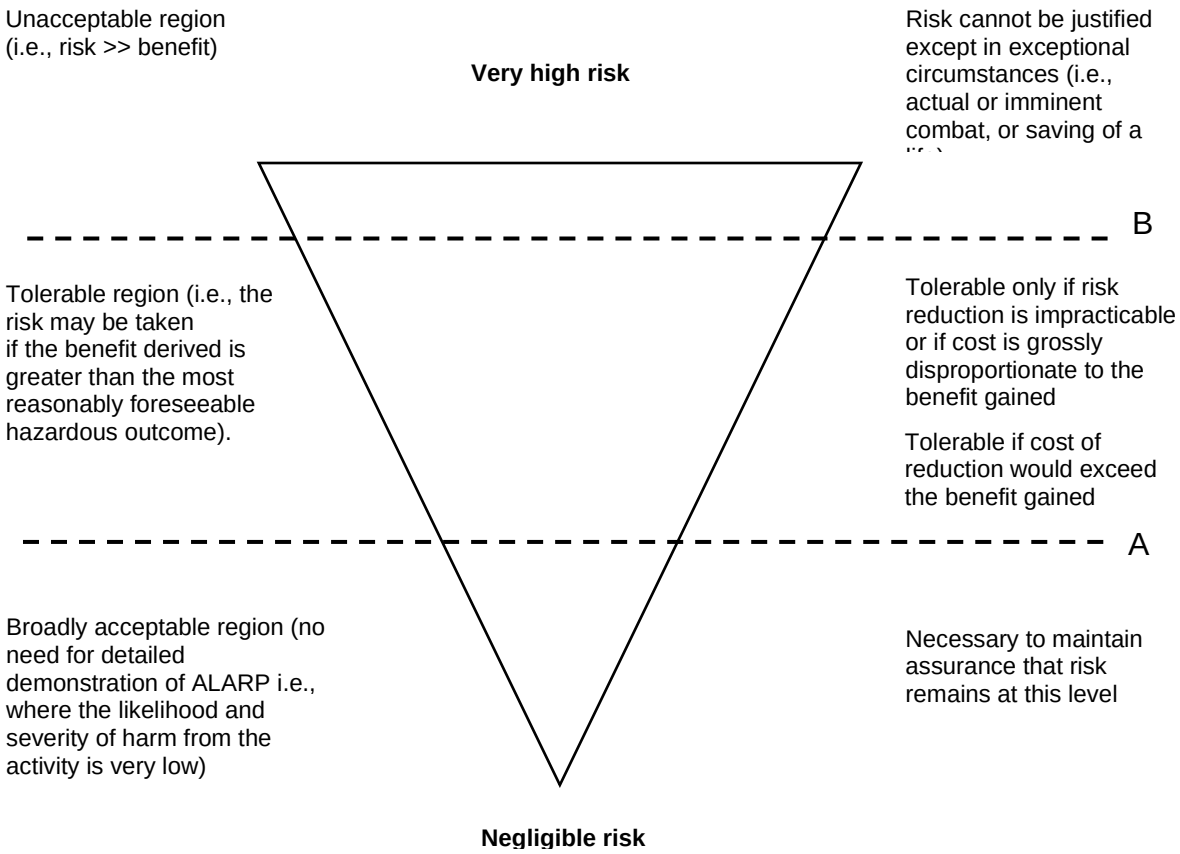

Figure 1 – Risk tolerability framework

16. “It must be stressed that Figure 1 is a conceptual model. Moreover, the factors and processes that ultimately decide whether a risk is unacceptable, tolerable or broadly acceptable are dynamic in nature and are sometimes governed by the particular circumstances, time and environment in which the activity giving rise to the risk takes place. For example, standards change, public expectations change with time, what is unacceptable in one society may be tolerable in another, and what is tolerable may differ in peace or war. Nevertheless, the protocols, procedures and criteria described in this document should ensure that in practice, risks are controlled to such a degree that the residual risk is driven down the tolerable range so that it falls either in the broadly acceptable region or is near the bottom of the tolerable region, in keeping with the duty to ensure health, safety and welfare so far as is reasonably practicable”. (HSE Reducing risk, protecting people)

Change management risks

17. All significant changes to equipment or infrastructure (including major software changes) and associated specifications must be evaluated, risk assessed, approved and documented prior to implementation. Defence organisations must risk assess the proposed change using competent people with the relevant Skills, Knowledge, Experience, Behaviours (SKEB). The term Suitably Qualified and Experienced Personnel (SQEP) is a widely recognised term used, but the meaning behind them both is the point about a person being competent.

18. Continuous monitoring and safety reviews should be conducted throughout the change implementation phase, feedback and lessons learned should be recorded, reviewed by the leadership and actions tracked to completion for the benefit of continual improvement. For organisational changes, the impacts of the proposed change should be assessed by undertaking an Organisational Safety Assessment (OSA).

19. Change management risks and OSAs are covered more in Element 2 of this Volume 2.

Safety cases

20. If work-related Defence activity takes place on or involves a complex system (for example an aircraft, ship or weapon system) a simple risk assessment may not be sufficient to demonstrate that the risks have been adequately controlled. The use of a safety case provides the ability to understand the cumulative or interrelated risks from the use of the complex system and for this to be captured in a body of evidence. Safety cases should be developed in the initial stages of acquiring capability (when it is easier and less costly to avoid or mitigate safety risks) and maintained while the capability is in-service and being disposed of. Further information regarding safety cases is set out in the “White Booklet”[2], ASEMS[3] and the regulations for different Defence domains published by the Defence Safety Authority (DSA). Equipment safety and safety cases are covered more in Element 7 of this Volume 2 and JSP 376 Defence Acquisition Safety Policy.

[2] An Introduction to System Safety Management in the MOD, https://www.gov.uk/government/publications/safety-booklet-white-booklet

[3] The DE&S Acquisition Safety and Environmental Management System, https://www.asems.mod.uk/

21. The Defence organisation creates and maintains safety cases for the acquisition lifecycle for all activities and equipment requiring them. Safety cases are either owned by the Senior Responsible Person (SRO) or the User and independently assured. Industrial partners give relevant support. Stakeholder engagement should be undertaken for both safe to operate and operate safely aspects.

22. A safety case is to be:

a. proportionate to the risks which the system poses and are readily accessible to the workforce;

b. understood by the operators and training given to them to provide that knowledge where appropriate;

c. regularly reviewed, endorsed by the SRO or User;

d. certified throughout the lifecycle of the acquisition lifecycle of the system; and

e. concurrently assured under the 3LOD Model (see Element 12) by internal regulators (DSA) and external assurers (Infrastructure and Projects Authority (IPA)) if required by further Defence policy (for example JSP 655 – Defence Investment Approvals) or wider Government policy.

23. Each potential acquisition strategy may have a different safety philosophy and safety case. Different approaches may be appropriate depending on whether capability is being acquired as a standalone product, an integrated system or platform, or as a managed service. Whatever approach is taken, the safety case for the capability should cover the whole service and not just the equipment design.

Methods of risk management

24. Defence organisations should identify and manage their safety risks in a consistent, rigorous and technically robust way. There are various approaches for identifying and managing risks, however the approach recommended by the Director DS for safety risks is the bow-tie method.

25. The bow-tie method is a visual tool that diagrammatically represents the different elements of a safety risk so that it can be viewed in a risk picture which is shaped like a bow-tie as shown in Figure 2. Further details on the bow-tie and other methods of risk identification and management can be found in JSP 892 (Risk Management).

Figure 2 – Bow-tie illustration

Risk matrices

26. Risk matrices are a tool used to help codify risks and to assist in the decision of how they are to be managed. A risk matrix categorises risks according to their severity and likelihood. Each cell in the matrix is assigned a category or classification. This allows different risks to be compared, e.g., to show that a high-likelihood, low-severity risk can be considered to have the same importance as a low-likelihood, high-severity risk. The distinct categories can also correspond to different management treatments, e.g., to indicate the level of authority required to allow a certain level of risk to be tolerated.

Risk reporting – Defence organisation level

27. Defence organisations are required to maintain safety risk matrices.

28. The 5 x 5 risk matrix template in MOD Form 5010 is the recommended matrix for categorising risks according to their severity and likelihood. This matrix uses a likelihood scale based on the number of risk events per year across the organisation and a severity that denotes the outcome that the risk would have if it materialised.

29. When reviewing risks across an organisation, a common matrix is needed to enable consistent analysis, comparison, and aggregation of safety risks.

30. Defence organisations may use other safety risk matrices with the size and axes scales decided by them to suit their individual circumstances (nature and diversity of risks held and risk appetite). When risk matrices are used to support workplace risk assessments or safety cases, they should be calibrated to suit the magnitude of harm likely to be presented (severity) and to allow the likelihood to be estimated easily. Likelihood scales might be calibrated according to the expected number of risk events ‘per year,’ ‘per km driven,’ ‘per sortie,’ or ‘per round fired,’ etc. to allow easy comparison with occurrence data and appropriate standards for the type of work or the system being used.

Risk reporting – corporate level

31. The Defence Safety and Environmental Committee (DSEC) have directed that safety risks must be presented to the DSEC in a common risk matrix to enable consistent analysis and comparison. As such Defence organisations must use the 5 x 5 risk matrix at Figure 3 when presenting their most serious risks to life at the Defence level to the DSEC or the quarterly Defence Board. The 5 x 5 risk matrix is aligned to the risk matrix in JSP 892 Risk Management.

32. It is the Defence organisation’s responsibility to transpose their top 8 safety risks from their individual risk matrices onto the common 5 x 5 safety risk template at Figure 3 and to provide an accompanying narrative. The narrative should briefly summarise the nature of and management approach to the risk and any pertinent details for the DSEC’s attention, including the assumptions made when transposing from the Defence organisation’s own matrix for example, the number of people exposed, the number of systems deployed, or the level of activity expected during a year.

33. Defence organisations must decide upon and maintain their top 8 safety risks (which may lead to a risk to life). It is recognised that Defence organisations may be managing more than 8 safety risks, however the focus for reporting at DSEC will be on the top 8 safety risks. These top 8 safety risks must be reviewed and agreed by the most senior leader in each Defence organisation.

34. The safety risk associated with each of these top 8 safety risks must be quantified in terms of likelihood and severity. The likelihood must be based on the estimated frequency at which the safety risk is expected to materialise. The severity must be defined in terms of the severity of injury or loss of life and potential number of lives impacted in one event. The DDS will maintain a 5 x 5 risk matrix in the format of the safety risk matrix template at Figure 3 which will be used to communicate the Defence top 8 safety risks to both the DSEC and the Defence Board.

35. Defence organisations must review their top 8 safety risks at least annually and provide these to the Director DS. Where a Defence organisation owns one of the Defence top 8 safety risks, an update must be provided quarterly to the Director DS to inform Defence Board Quarterly Risk Reporting.

Risk Matrix - Guidance

36. The 5 x 5 safety risk matrix is used to plot the severity of a risk against the likelihood of a risk occurring. JSP 892 is the source of the 5 x 5 safety risk matrix however the x-axis of the template of Figure 3 has been adapted from percentages, which are more appropriate for calculating business and financial risks, to a 'calendar year' time period which is more appropriate for safety risks. To calculate the risk rating, please use the definitions of severity as defined in Table 1 and likelihood as defined in Table 2.

Severity (the terms Impact and Consequence can also be used) - Choose the level of severity found on the vertical (y-axis) on the left-hand side of the matrix. This denotes the severity of the outcome, that the risk would have if it materialised. The following table provides the definitions of severity, the full details of the MOD Risk Assessment Impact Criteria are set out in JSP 892 Risk Management, Part 2 Guidance, Appendix A.

Severity (y-axis)	Definition
Critical	Multiple fatalities.
Severe	• Single fatality • Specified injuries to multiple individuals (which are life threatening and / or cause permanent disability).
Major	• Single specified injury (which is life threatening and / or causes a permanent disability). • Specified injuries to multiple individuals' injuries of a non-life threatening, non-permanent nature and/or have a short-term impact on normal way of/quality of life.
Moderate	Specified injuries to multiple individual's injuries of a non-life threatening, non-permanent nature and requiring first aid only.
Minor	Single specified injury of a non-life threatening, non-permanent nature and requiring first aid only.

Table 1 - Severity definitions

37. **Likelihood** (the terms frequency or probability can also be used) - Choose a descriptor, found on the horizontal (x-axis) on the bottom of the matrix. This denotes the likelihood that the safety risk will occur and thus become an event. The likelihood is based on the estimated frequency in calendar years at which the safety risk is expected to materialise, across the whole of the Defence organisation's area of responsibility.

Likelihood (x-axis)	Definition
Very likely (Very high)	1 or more events per year
Likely (High)	1 or more events per 10 years
Possible (Medium)	1 or more events per 25 years
Unlikely (Low)	1 or more events per 50 years
Very unlikely (Very low)	1 or more events per 100 years

Table 2 - Likelihood Definition

Note: Where a safety risk is to be plotted beyond the scale of the common matrix this must be explained in the accompanying narrative. Such a risk should be plotted on the edge of the matrix, for example where a risk has a likelihood of 1 per 1,000 years or less then it would be plotted on the left-hand edge of the y-axis.

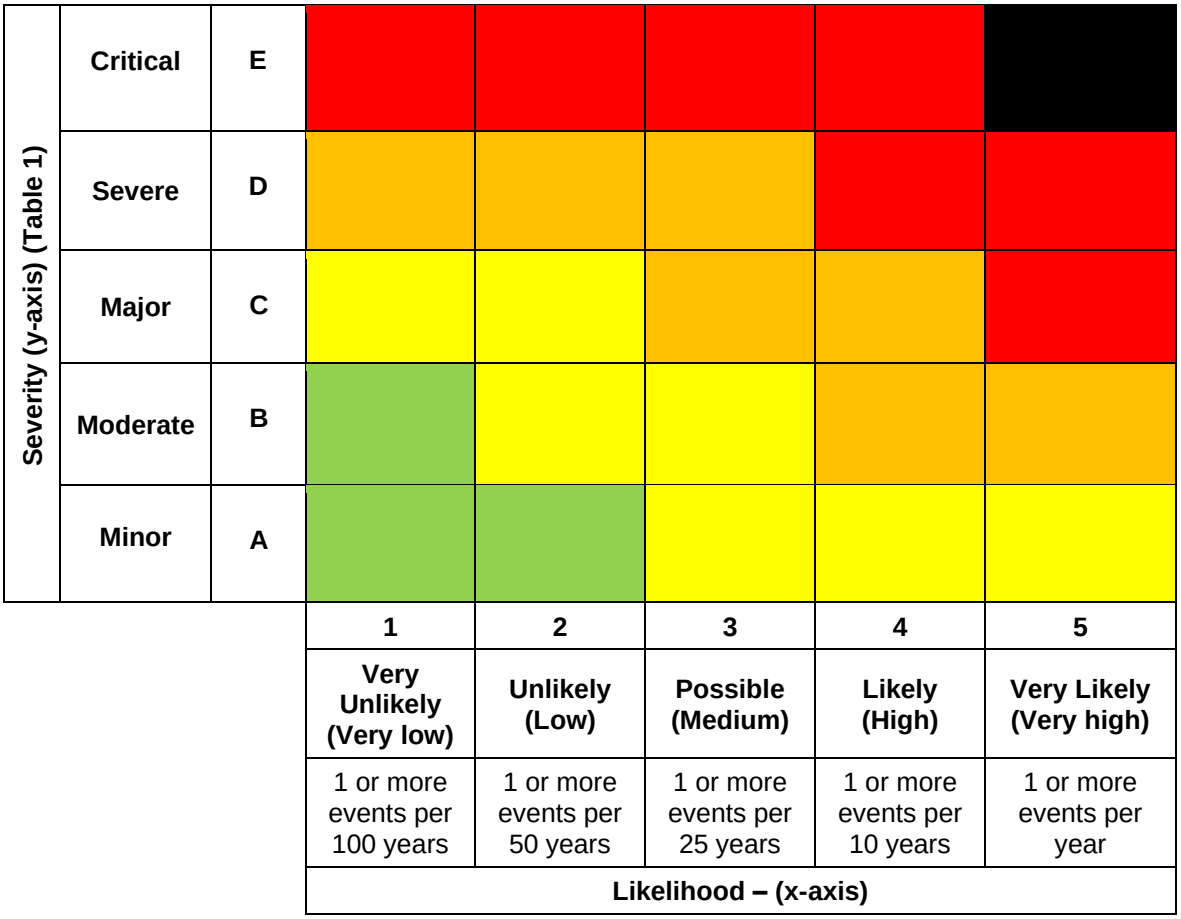

Figure 3 - Safety 5 x 5 risk matrix

Very High	Rigorous scrutiny of control measures required to make sure risk is ALARP and then make sure it is tolerable, by improved control measures; stop work unless those rare occasions when continuation is justified as essential to delivering a military task (urgent operational imperative). Tolerating this level of risk to conduct activity requires formal consideration and acknowledgement from the appropriate most Senior Leader, Duty Holder or nominated Responsible Person who is charged with Risk Ownership.
High	Rigorous scrutiny of control measures required to make sure risk is ALARP and then make sure it is tolerable, improve control measures where possible; consider stopping work unless continuation is justified as essential to a military context. Tolerating this level of risk to conduct activities will require formal consideration and acknowledgement from the appropriate Duty Holder, Commander, Head of Establishment or nominated Responsible Person who is charged with Risk Ownership.
Medium	Review control measures and improve if reasonably practicable to do so, consider alternative ways of working. Consider informing command chains of any changes and requesting additional resource / levers / authority to apply additional controls that may reduce the residual risk further.
Low	Maintain control measures and review regularly or if there are any changes that may impact either Severity or Likelihood.
Very Low	Maintain control measures and review at least annually to ensure that any changes to the residual risk, or effectiveness of controls are not re-introducing a credible RtL or potential Environmental impact.

Table 3 - Risk Assessment Actions

Element summary

38. Defence leaders are to ensure their organisation:

a. Have mechanisms in place to assess its risk profile and identify its safety hazards.

b. Have mechanisms in place to manage its safety risks, including provision of proportionate controls.

c. Assess risks and where safety risks are significant, these risks are elevated, and leadership are actively involved in their management.

d. Have arrangements in place to communicate safety risk to all stakeholders, outlining control measures needed to provide safe working practices.

e. Have mechanisms in place to continually improve risk management with the aim of eliminating fatalities whilst enhancing Defence capability and minimising injury.

f. Tracks changes, such as those impacting equipment, operations, infrastructure, training, people, plans and procedures, and takes action to manage associated risk.

g. A safety case is maintained throughout the acquisition lifecycle that identifies, evaluates, and manages the risk from concept development through to disposal.