Ministry of Defence

JSP 815

Element 4: Risk Assessments and Safety Cases

Contents

Title	Page
Amendment record	1
Terms and definitions	1
Introduction	2
Purpose and expectations	2
Management and assessment of safety risk	2
Risk mitigation	4
Elevating safety risks	6
Change management risks	6
Safety cases	7
Methods of safety risk management	8
Element assurance framework	14
Expectations and performance statements	15

Amendment record

JSP 815 has been updated as a part of Defence Reform and will be subject to further scheduled reviews and updated as required.

This Element has been reviewed by the Directorate of Defence Safety & Support (DDSS) together with relevant subject matter experts and key Safety stakeholders. Any suggestions for amendments **should** be sent to People-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 Jun 23	Final version	DDS
1.2	10 Sep 24	Annual revision and combined Element and assurance framework	DDS
1.3	1 Sep 26	Scheduled revision and Defence Reform update	Dir-DSS

Terms and definitions

The term ‘Defence Area’ refers to one of the four top-level areas of Defence: Department of State (DOS), Armed Forces (MSHQ and Military Commands), National Armaments Director (NAD) Group and the Defence Nuclear Enterprise (DNE). Within Defence Safety Policy (JSP 815, JSP 375 and JSP 376), reference to a ‘Defence Area’ responsibility applies to the top-level Defence Area however, for the Armed Forces it also applies to their component Military Commands (Army, Air, Navy and CSOC).

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

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.

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 this Element 4.

Purpose and expectations

2. This guidance supports Defence Areas 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, to demonstrate that risks are being managed and that appropriate controls are in place to achieve a safe system of work.

Management and assessment of safety risks

Risk management

3. The Health and Safety at Work etc. Act (HSWA) 1974, Section 2, places general duties on employers for their employees so that 'it shall be the duty of every employer to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all of their employees and, under Section 3, anyone else who may be affected by that work activity.

4. There is also a duty on employers under the Management of Health and Safety at Work Regulations (MHSWR) 1999 to carry out a suitable and sufficient assessment of the risks to the health and safety of their employees[1]. As such, Defence requires commanders, managers and accountable persons to make sure that suitable and sufficient risk assessments are carried out in order to mitigate health and safety risks to the personnel under their area of responsibility and anyone else who may be affected by that work activity. Defence safety risk assessments must be carried out in accordance with Chapter 8 of JSP 375: Management of Health and Safety in Defence.

5. Safety risk management in Defence must be conducted in accordance with this JSP and JSP 892. Defence Areas should be able to demonstrate how effective safety risk management is incorporated into their safety management arrangements and that a safety risk management framework is in place. The safety risk management framework is owned by the senior leader within the Defence Area 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.

[1] Regulation 3 – Risk assessment

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

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. where risks are a higher level than the commander or manager is authorised to accept, including reasonably foreseeable risks to life (RtL), they must be elevated in line with their Defence Area's elevation process to determine the appropriate level of risk ownership.

Risk profile

7. The risk profile is the examination of the safety 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; and

d. The effectiveness of control measures in place.

8. Defence Areas must establish their own risk profile for assessing and managing their safety risks. A Defence Area's risk profile must 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.

Safety risk assessment

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

10. Defence Areas must make sure that suitable and sufficient safety 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.

11. Defence Areas must have an effective process in place to communicate the safety risks and associated control measures to all relevant stakeholders, to provide safe working practices. This should include TU safety representatives, and other workforce representatives where applicable. Communication of safety risks and control measures should be accessible to all personnel and should take account of differing communication needs, working environments and accessibility requirements.

Risk mitigation

Reducing risks to ALARP

12. The HSWA uses the term 'So Far As Is Reasonably Practicable' (SFAIRP), for general safety duties often emphasising the 'legal duty' to act in a way that demonstrates that all reasonable steps have been taken against the cost (in terms of money, time, and effort). Defence more commonly uses the term As Low As Reasonably Practicable (ALARP) in safety risk management for emphasising the 'process' of lowering the risk to a level that is ALARP. Both terms are based on the concept of doing what is 'reasonably practicable.

13. When a risk is considered ALARP, this is when the risk has been reduced to a level where applying further control measures would be grossly disproportionate to the benefit that would be gained. The application of managing safety 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 (money, time, and effort) needed to control the risk.

14. To demonstrate that a safety 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 safety risk is mitigated to ALARP there may still be a high residual risk remaining.

15. Reducing safety risks to ALARP is achieved through undertaking a suitable and sufficient safety risk assessment and implementing the control measures identified in the risk assessment. Control measures must be identified and implemented in accordance with the hierarchy of controls which is set out in Chapter 8 of JSP 375 Volume 1. For systems that are more complex a single safety risk assessment may not be sufficient to demonstrate that all the safety risks have been reduced to ALARP and therefore a safety case may be required; safety cases are covered in more detail further on in this Element. It may also be necessary to apply enhanced management oversight to certain activities to maintain the effectiveness of arrangements and ensure a timely and appropriate response to changes (including organisational changes).

Risk tolerability

16. In addition to a risk being reduced to a level where it is considered to be ALARP, the tolerability of the risk also needs to be considered, and an evaluation made as to whether the risk can be tolerated (accepted). Risk tolerability is a level of risk that we are willing to accept in order to perform an activity or achieve an outcome. A tolerable risk is one that is considered to be worth taking, if it has been evaluated and is being managed. Once the risk has been reduced to ALARP and the tolerability decision has been made to accept the risk, it can then be considered as being ALARP and tolerable.

17. The concept of tolerability is generally applied to higher risk activities and whether the risk of injury or fatality within a workforce or wider society can be tolerated. Under most circumstances a risk is considered as being tolerable when the cost (money, time and effort) of further risk reduction is grossly disproportionate to the safety benefit. The tolerability boundary is defined as being between a risk that we are willing to accept (and the conditions under which we are willing to accept it) or an unacceptable risk. The tolerability boundaries may change depending upon the operating circumstances, this is identified by the lines A and B of the conceptual model shown at Figure 1 of this Element.

18. 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, set against the Defence benefit derived from the activity. 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 policy should ensure that in practice, risks are controlled to such a degree that the residual risk is driven down to as low in the tolerable zone as practicable, in keeping with the duty to ensure, so far as is reasonably practicable, the health, safety and welfare of personnel.

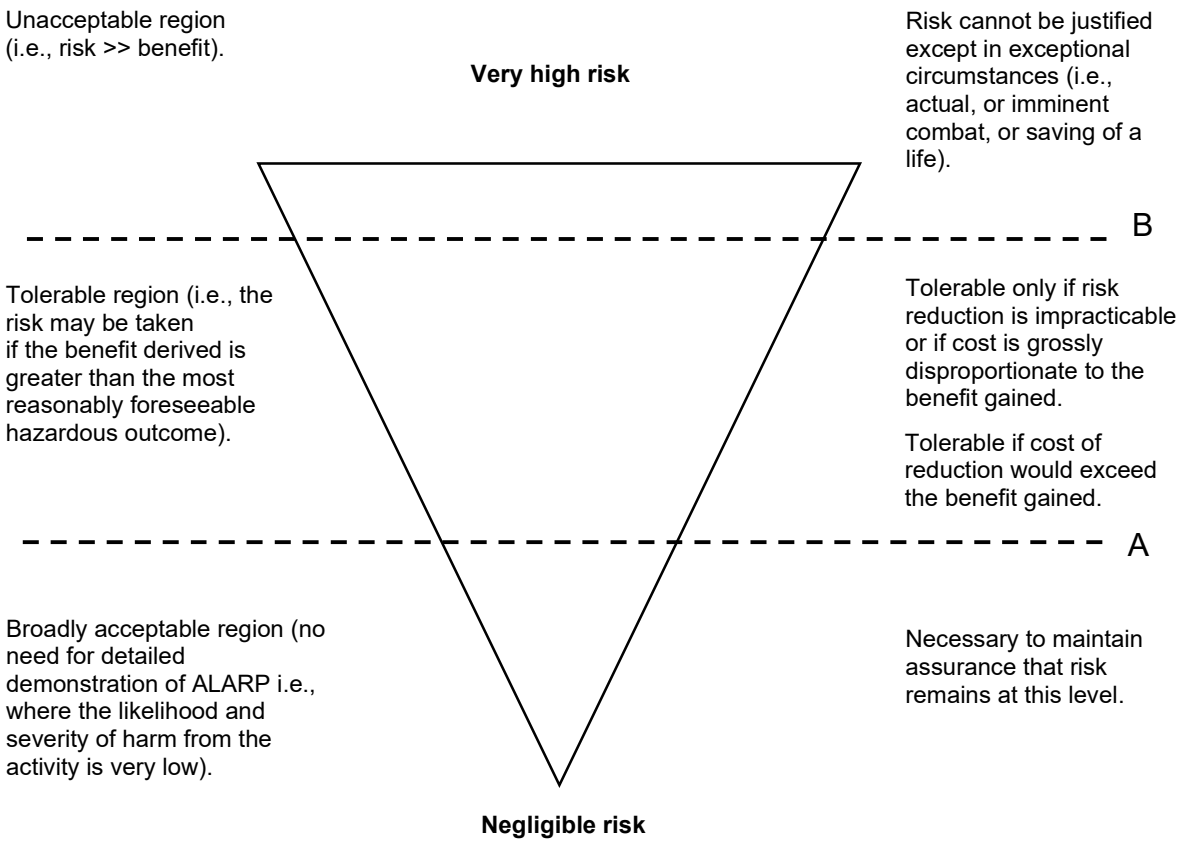

Figure 1 – Risk tolerability framework

Elevating safety risks

19. Those responsible for the control of activity must have clear and accessible mechanisms such as the risk management framework, safety committees, risk registers and elevation pathways in place to assess safety risks and elevate them when they exceed their authority, competence, or available resources to ensure that leadership is informed of emerging or deteriorating risks. Elevation processes should be embedded within organisational procedures, work instructions, and orders, ensuring that individuals understand when and how risks should be elevated.

20. Effective safety risk management relies on timely elevation of risks that exceed the authority, competence, or resources of those directly responsible for the activity. When a risk cannot be controlled to a level that is ALARP and tolerable, or when uncertainty exists about the adequacy of the current control measures in place, the risk **must** be elevated through the appropriate chain of command.

21. Elevation enables senior leaders to exercise appropriate oversight, allocate resources, provide direction, or make risk acceptance decisions.

22. Elevation should occur when existing controls are no longer effective or proportional, and the activity presents an increased potential risk of injury or has strategic safety implications.

a. The likelihood or severity of a risk has increased based on new information, operational changes, or occurrence data.

b. The decision to accept or tolerate a risk sits above the level of authority the person conducting or supervising the activity is authorised to accept.

23. Leadership must be actively involved in the management of elevated risks. Defence Areas must ensure that elevated risks are reviewed, acted upon, and tracked, and that lessons learned are used to strengthen both the mechanisms for elevation and the overall safety risk management process. Robust governance arrangements should demonstrate that elevation procedures are routinely communicated, monitored for effectiveness, and continually improved.

24. Throughout the elevation process records should be maintained to provide an audit trail of decision making and rationale. All decisions should be proportionate to the severity of the risk, and they should be promptly actioned. This approach ensures a coherent “golden thread” of safety risk communication, maintains organisational awareness of significant risks, and supports the Defence objective of eliminating fatalities, enhancing capability, and minimising injury.

Change management risks

25. All significant changes to equipment, infrastructure or ways of working (including electronic ways of working) and associated specifications must be evaluated, risk assessed, approved and documented prior to implementation, further information on this can be found in Chapter 35 (Safety and the management of change) of JSP 375, Volume 1.

26. Defence Areas must risk assess the proposed change using competent people with relevant Knowledge, Skills application, Experience, Behaviours (KSEB). The term Suitably Qualified and Experienced Personnel (SQEP) is a widely recognised term used, but the meaning behind them both is that the person(s) conducting these assessments are competent to do so.

27. 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. Consideration should be given to any impacts on workforce health, safety, wellbeing, inclusion, accessibility, and the ability of personnel to safely undertake their duties following changes.

28. Organisational changes (for example changes to the organisation structure or to personnel with specific KSEB) should be assessed and where proportionate to do so the change owner must decide whether an Organisational Safety Assessment (OSA) needs to be conducted.

29. Change management risks and OSAs are covered more in Element 2 of this JSP and Chapter 35 (Safety and the management of change) of JSP 375, Volume 1.

Safety cases

30. A safety case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible, and valid justification that a system is safe for a given application within a defined operating environment.

31. A safety case is required where Defence work-related activities are conducted on, or form part of, a system[2] where a single safety risk assessment for the activity or the workplace is not sufficient to demonstrate adequate risk control (due to the complexity, novelty, scale, or the risk profile). A system may comprise of equipment, infrastructure, people, processes, organisational arrangements, or any combination of these, including how they are integrated and how they interact.

32. A safety case is not required for simple, (non-complex, routine) activity. Where risks can be adequately managed to a level that is ALARP and tolerable through suitable and sufficient risk assessments and Standard Operating Procedures (SOPs) / work instructions, those arrangements remain the primary means of risk control. Safety cases should be reserved for systems where complexity, integration, novelty, or uncertainty requires a structured demonstration that risks have been reduced to ALARP and are tolerable.

Note: For equipment safety cases, refer to Element 7 of JSP 815 and JSP 376 - Defence Acquisition Safety Policy .

[2] A system is defined in Def Stan 00-056 as “a combination, with defined boundaries, of elements that are used together in a defined operating environment to perform a given task or achieve a specific purpose. The elements may include personnel, procedures, materials, tools, products, facilities, services and/or data as appropriate.”

33. The safety case provides the means to demonstrate that the system safety risks have been identified, assessed, and managed to a level that is As Low As Reasonably Practicable (ALARP) and tolerable. It shows that appropriate controls are in place to support a safe system of work. A safety case brings together a holistic view of cumulative and interrelated risks into a single, coherent body of evidence and is distinct from routine safety risk assessments which are described in more detail in Chapter 8 of JSP 375, Volume 1.

34. The scope and complexity of a safety case should be proportionate to the level of risk and system complexity, it may range from a single equipment safety case to a broader safety case incorporating multiple equipment safety cases and activity and / or workplace risk assessments, as illustrated in Figure 2. Defence Areas may use other terms to describe a safety case for a system (such as a safety management plan), but the basic principle is to demonstrate that appropriate controls are in place to support a safe system of work. Equipment safety cases are addressed in more detail in Element 7 of this JSP and in JSP 376 - Defence Acquisition Safety Policy.

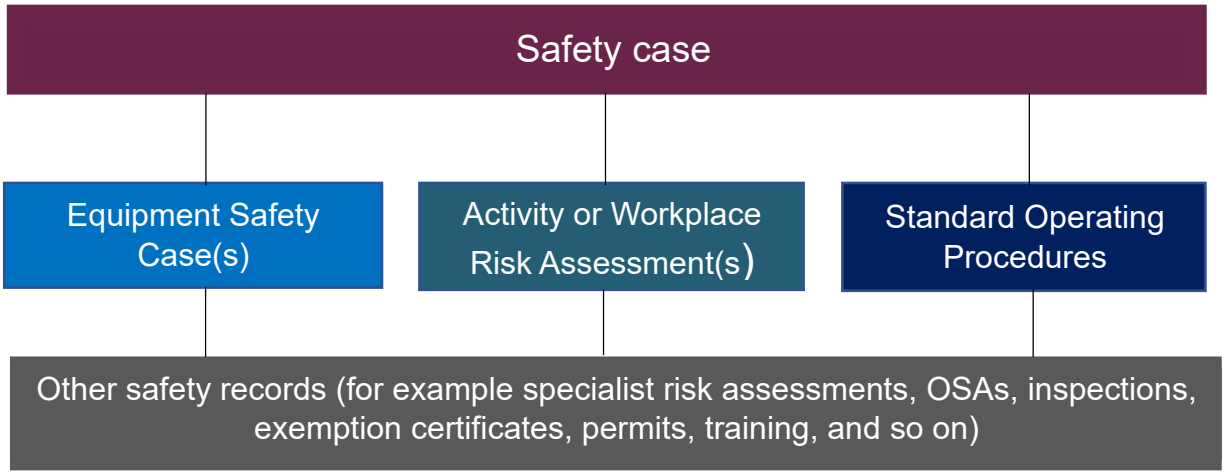

Figure 2 – Safety case composition

Methods of safety risk management

35. Defence Areas should identify and manage their strategic safety risks in a consistent, rigorous, and technically robust way. There are various approaches for identifying and managing strategic safety risks, however the approach recommended by the Director of Defence Safety & Support (Dir-DSS) is the bow-tie method.

Bow-tie Method

36. The bow-tie method is a simple visual approach used to identify, manage, and communicate safety risks by mapping the pathways from potential causes to possible consequences. It places a hazard and “top event” (the moment a hazard is realised) at the centre, with threats or causes on the left and consequences on the right forming a diagram shaped like a bow-tie (as shown in Figure 3). Preventive controls are positioned on the left to stop threats from leading to the event, while mitigation or recovery controls are positioned on the right to reduce the impact if the event occurs.

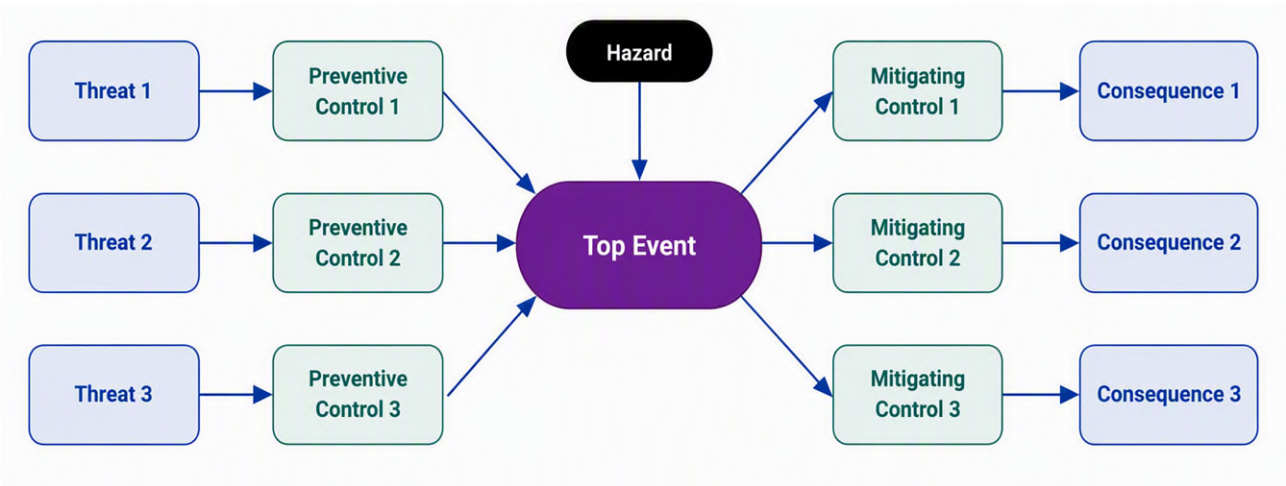

Figure 3 – Bow-tie illustration

37. Further details on the bow-tie and other methods of risk identification and management can be found in JSP 892 (Risk Management).

Risk matrices

38. Risk matrices are a tool used to help codify risks and to assist in the decision of how they should 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 managed against their corresponding risk rating (Table 3). The distinct categories can also correspond to different management treatments for example, to indicate the level of authority required to allow a certain level of risk to be tolerated.

Risk reporting – Defence Area level

39. Defence Areas must maintain safety risk matrices and the recommended Defence 5 x 5 safety risk matrix is defined below in the Risk Matrix - Guidance section. 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.

40. Use of the Defence 5 x 5 safety risk matrix provides Defence with a standard way of presenting safety risks and enables consistent analysis, comparison, and aggregation of those risks. Where safety risk reporting methods differ, the relevant Defence Area must define their methodology within their respective safety management arrangements.

41. When risk matrices are used to support workplace safety 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 are generally calibrated according to the expected number of safety risk events per year, and this must be the case for reporting at strategic level, although other scales or time periods could be used for assessing and measuring risks at a more local level.

Risk reporting – Strategic level

42. The Defence Board oversees risk management in MOD and agrees the Principal Risks. The safety function through the Dir-DSS reports on the safety Principal Risks.

43. The Principal Safety Risk[3] is generated from the accumulation of numerous strategic safety risks. The strategic safety risks are generated from the Defence Area / organisation high scoring and / or accumulation of safety risks. The DDSS identifies strategic Safety Function risks which are those that are sufficiently serious or those captured on multiple organisations' risk registers and hence are deemed to be pan-Defence. Individual Areas capture and report activity strategic safety risks to their Area Management Board. The strategic safety risk reporting framework is shown at Figure 4.

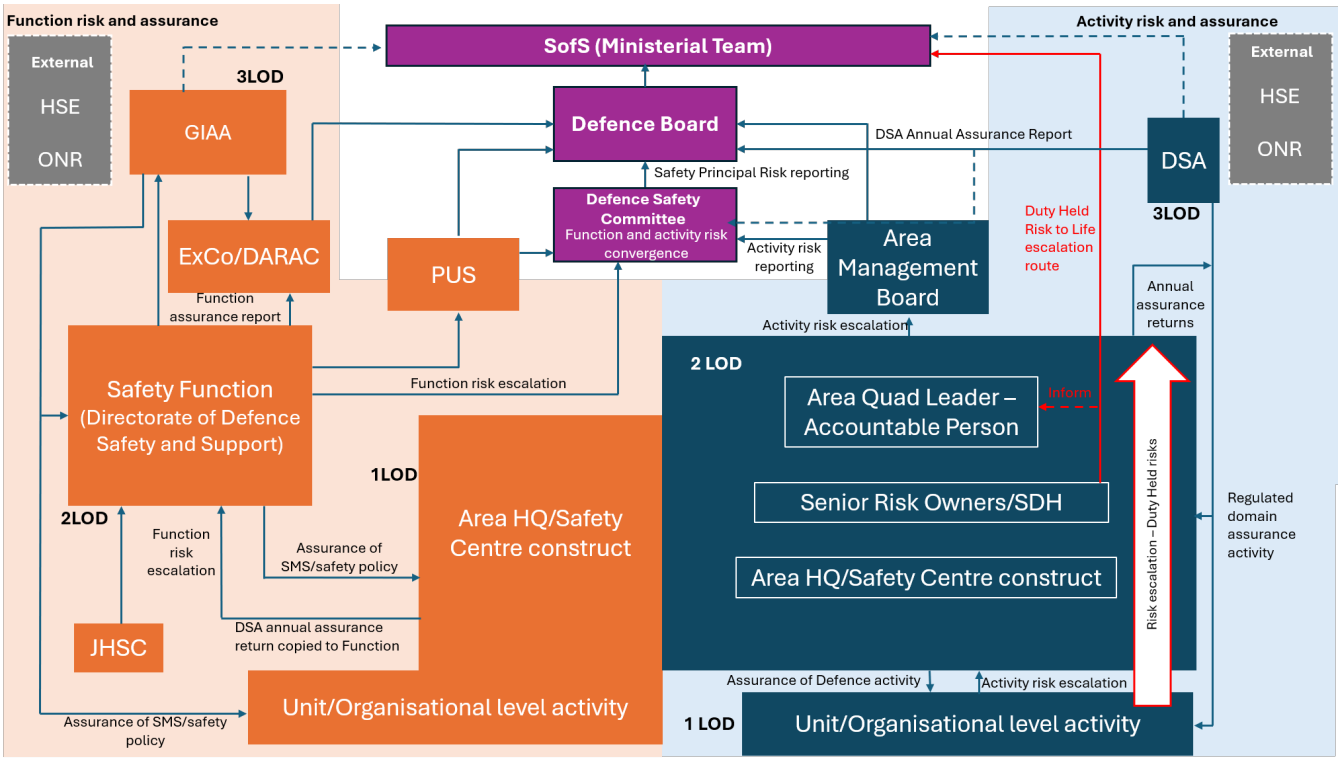

Figure 4 – Strategic safety risk reporting framework

44. Figure 4 sets out how Safety Function risk (orange) and Activity safety risks (blue) are reported and assured, including the exceptional elevation route for time critical Duty Held risk.

45. Defence applies a Three Lines of Defence model as set out in the Defence Safety Function Operating Model to provide layered assurance over:

a. Activity risk and assurance (managed by the Defence Areas and delegated to the appropriate level within those Areas; assured via Area constructs, DDSS and the DSA), and

b. Safety Function risk and assurance (owned through the safety function, aligned to the Orange Book).

[3] A principal safety risk is a risk or combination of safety risks that can materially impact Defence's ability to achieve its critical objectives, affecting its performance or reputation.

46. As part of the safety function risk reporting, Defence Areas must regularly provide a report against strategic function safety risks to the DDSS. The report must provide the required information captured by the Defence Area. The report must include their risk scoring as well as outlining their control and mitigation measures. Defence Areas will also be asked to:

a. highlight to the DDSS's attention any new and emerging safety risks not already identified as one of the existing strategic safety risks; and

b. highlight specific safety function risk issues and impacts they wish to be highlighted in the supporting safety function narrative and forward reporting.

47. Defence Areas should report strategic level function and activity safety risks using the Defence 5 x 5 safety risk matrix.

48. DDSS will collate updates against the strategic and principal risks for submission to the Defence Safety Committee (DSC), through the Department of State Management Board, and through the Executive Committee (ExCo) to the Defence Board and in addition, through the Defence Risk and Assurance (DRA) and Defence Audit and Risk Assurance Committee (DARAC) to the Defence Board.

49. Defence Areas must monitor function and activity safety risks (including but not limited to risk to life). Defence Areas may be managing multiple strategic safety risks, however the focus for central reporting will be on the risks that the Defence Area deems to be of significant importance to raise to the DSC or Defence Board. These top strategic safety risks must be reviewed and agreed by the most senior leader in each Defence Area.

50. The safety risk associated with each of these strategic 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.

51. Defence Areas must review their top strategic safety risks at least quarterly for their Defence Area Management Boards and provide this risk data to the DDSS Risk & Insights team in order to inform the Dir-DSS through principal risk reporting to ExCo and to the Defence Board when appropriate. This ensures the 'Golden Thread' risk reporting process is in place.

52. The Dir-DSS will collate Safety Function risks based on the analysis and risk returns from Areas, inform the DSC and Defence Board of Safety Function risks, which are included as part of the safety Principal risk reporting.

Risk Matrix - Guidance

53. The 5 x 5 safety risk matrix is in line with the JSP 892 risk matrix used to plot the severity of a risk against the likelihood of a risk occurring, however the x-axis and y-axis of the template of Figure 5 have been adapted from percentages, which are more appropriate for calculating business and financial risks, to a format more appropriate for safety risks. To calculate the risk rating, use the definitions of severity as defined in Table 1 and likelihood as defined in Table 2.

Severity (y-axis)							
	Critical	E					
	Severe	D					
	Major	C					
	Moderate	B					
	Minor	A					
			1	2	3	4	5
			Very Unlikely	Unlikely	Possible	Likely	Very likely
			Likelihood (X-axis)				

Figure 5 – Safety 5 x 5 risk matrix

54. **Severity** (the terms Impact and Consequence can also be used) - Choose the descriptor 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, based on the example of personal injury categories. Further information can be found in Chapter 16 (Safety Occurrence Reporting and Investigation) of JSP 375 Volume 1, into aligning the reporting of these and other factors such as equipment or infrastructure damage.

Severity (y-axis)	Definition
Critical (E)	Multiple fatalities.
Severe (D)	• Single fatality • Specified injuries to multiple individuals (which are life threatening and / or cause permanent disability).
Major (C)	• 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 (B)	Single specified injury (which is non-life threatening, non-permanent nature and / or has a short-term impact on normal way of / quality of life). Single injury / illness of a non-specified injury (for example moderate heat illness or hypothermia) requiring more than just first aid
Minor (A)	Single injury of a non-specified or non-life threatening, non-permanent nature and requiring first aid only.

Table 1 – Severity definitions

55. **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 probability that the safety risk is expected to materialise. Generally, it would be per calendar year, this metric must be used for strategic level reporting, however at Defence Area level reporting, other likelihood scales may be used locally or by the relevant DSA regulator as defined in their documentation.

Likelihood (x- axis)	Probability	Description
Very likely (5)	>75%	Is or is likely to be a common occurrence.
Likely (4)	50% - 74%	Has occurred or is likely to occur many times (more than several but not yet considered as a common occurrence).
Possible (3)	30% - 49%	Has occurred or is likely to occur on several occasions.
Unlikely (2)	5% - 29%	Has occurred or is likely to occur on a small number of occasions (more than once but less than several).
Very unlikely (1)	< 5%	Has occurred once / never or is not likely to occur.

Table 2 – Likelihood Definition

56. **Risk rating** - Is a measure of exposure to possible loss (or harm) and it combines the severity of loss (how bad) and the likelihood of suffering that loss (or harm) and (how often). The following key to the risk matrix provides the actions to be taken derived from the risk rating intersection (colour coding) of the x and y axis.

Very High	Rigorous scrutiny of control measures required to make sure the safety risk is ALARP and tolerable, improve control measures; stop the activity unless on the rare occasions continuation is justified as being essential to delivering a military task (urgent operational imperative). Tolerating this level of risk requires formal consideration and acknowledgement from the appropriate most Senior Leader, Duty Holder (if applicable) or the person who has been nominated as the risk owner.
High	Rigorous scrutiny of control measures required to make sure safety risk is ALARP and tolerable, improve control measures where possible; consider stopping the activity unless continuation is justified as essential in a military context. Tolerating this level of risk will require formal consideration and acknowledgement from the appropriate Duty Holder (if applicable), commander, manager, accountable person, or the person who has been nominated as the risk owner.
Medium	Review control measures to make sure they remain effective and if necessary, request additional resources and authority to apply additional control measures to make sure the safety risk is ALARP and tolerable. Tolerating this level of risk will require formal consideration and acknowledgement from the appropriate commander, manager, accountable person, or the person who has been nominated as the risk owner.
Low	Maintain control measures to make sure they remain effective, ALARP and tolerable and review regularly (at least annually) and monitor for any changes that may impact either 'severity' or 'likelihood.' Inform command chains if anything changes and if any further control measures are required to further reduce the risk.
Very Low	Maintain control measures to make sure they remain effective, ALARP and tolerable and review regularly (proportionate to the risk) to make sure that any changes to the residual risk, or effectiveness of control measure are not re-introducing a credible safety risk. Inform command chains if anything changes and if any further control measures are required to maintain the level of risk.

Table 3 – Risk Assessment Actions

Element assurance framework

57. The focus of this Element is to make sure that the Defence Area has put in place suitable and sufficient methods for identifying hazards and assessing risks as a basis of effective control of safety risk. Safety cases are routinely prepared and reviewed to verify that systems are being safely designed and used for their intended purpose in the correct operating environment.

58. The expectations and the performance statements for this Element are set out in the following pages.

Element 4: Risk Assessments and Safety Cases

The Expectations in this Element are:

E4.1 The Defence Area has mechanisms in place to assess its safety risk profile and identify its safety hazards.

E4.2 The Defence Area has mechanisms in place to manage its safety risks, including provision of proportionate controls.

E4.3 Those responsible for the control of activity have a mechanism in place to assess and elevate risk where necessary and leadership are actively involved in the risk management.

E4.4 The Defence Area has arrangements in place to communicate safety risk to all stakeholders, outlining control measures needed to provide safe working practices.

E4.5 The Defence Area has mechanisms in place to continually improve risk management with the aim of eliminating fatalities whilst enhancing Defence capability and minimising injury.

E4.6 The Defence Area tracks changes, such as those impacting equipment, operations, infrastructure, training, people, plans, and procedures, and takes action to manage associated risk.

E4.7 A safety case is developed, maintained and reviewed where required to demonstrate that safety risks associated with complex systems and activities are being managed to a level that is ALARP and tolerable.

Documents often associated with this Element:

- 1LOD assurance reports
- Agenda and minutes of the safety committee meetings (Strategic, Tactical and Working)
- Industry engagement (networking, conference, industry days)
- Change management process and plan
- Change risk register and examples of use
- Communications plan,
- Risk register
- Continual Improvement (CI) log and process
- Defence Area safety management arrangements
- Duty Holding construct and letters of delegation and acceptance
- Emergency arrangements and elevation process
- Industry engagement (Networking, Conference, Industry days)
- Incident reporting log
- Knowledge sharing forums
- Learning from Experience (LfE) communications
- Risk Returns
- Risk management plan including elevation process
- Risk to Life (RtL) register
- SLT risk review meeting minutes and actions
- Safety case log and tracker
- Safety case policy application and risk assessments
- Safety case reports and reviews
- Top eight (or another number) risks
- Workplace committees for Trade Union (TU) engagement and workers representatives)

Expectation 4.1 The Defence Area has mechanisms in place to assess its safety risk profile and identify its safety hazards.

Unsatisfactory	Limited	Moderate	Substantial
• Safety hazards and associated safety risk profile are not clearly defined or documented across the Defence Area.	• Safety hazards are identified but there is a limited safety risk profile. • A risk management framework is implemented within the Defence Area, but it is not routinely reviewed by leadership.	• Safety hazards are identified and there is a complete safety risk profile. • A risk management framework is applied across the Defence Area and regularly reviewed by leadership.	• Safety hazards are identified, and the safety risk profile is regularly reviewed. • A risk management framework is developed and used across the Defence Area; it is owned by leadership and used to drive continual improvement in safety performance.

Expectation 4.2 The Defence Area has mechanisms in place to manage its safety risks, including provision of proportionate controls.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence that risk assessments are used to develop effective controls to mitigate the risks associated with the Defence Area's operations.	• A process exists for using risk assessments to develop controls to mitigate risks, however it is not always applied effectively. • Risk assessments contain insufficient information and do not help the Defence Area implement and maintain proportionate controls.	• The Defence Area performs frequent risk assessments containing good information resulting in proportionate and relevant controls.	• Risk assessments consider the safety implications of wider risks and are frequently reviewed by leadership. • Proportionate controls are in place to mitigate risks and are developed through continual improvement.

Expectation 4.3 Those responsible for the control of activity have a mechanism in place to assess and elevate risk where necessary and leadership are actively involved in the risk management.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence to demonstrate that mechanisms in place for those responsible for the control of activity to assess and elevate risk. • There is little or no evidence to demonstrate that leadership is involved in risk management.	• There is some, but not enough evidence that those responsible for the control of activity have a mechanism in place to assess and elevate risk. There is some, but not enough evidence that it has been effectively communicated. • There is some, but not enough evidence that leadership is aware and involved in risk management.	• There is some but could be improved evidence that those responsible for the control of activity have a mechanism in place to assess and elevate risk. There is some but could be improved evidence that this has been effectively communicated, and included in work instructions, procedures, and orders, as necessary. • There is some but could be improved evidence that leadership is aware and involved in risk management.	• There is robust evidence that procedures to elevate risks are regularly monitored for effectiveness and lessons learnt and shared. Mechanisms in place are continually improved. • There is robust evidence that leadership is actively involved in risk management.

Expectation 4.4 The Defence Area has arrangements in place to communicate safety risk to all stakeholders, outlining control measures needed to provide safe working practices.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence to demonstrate that Governance, management, and communication arrangements of risk make control measures available to those who need them.	• Governance, management, and communication arrangements ensure that risks and control measures are available to and understood by those who need them, however there is some, but not enough evidence of information being frequently updated.	• Governance, management, and communication arrangements of risk ensure that those who need them are aware of updated risks and control measures.	• Governance, management, and communication arrangements ensure that feedback from the workforce is incorporated in risk control measures.

Expectation 4.5 The Defence Area has mechanisms in place to continually improve risk management with the aim of eliminating fatalities whilst enhancing Defence capability and minimising injury.

Unsatisfactory	Limited	Moderate	Substantial
• The Defence Area has little or no evidence of mechanisms for improved control of risks.	• The Defence Area has mechanisms in place to continually improve risk management, but there are significant weaknesses, and the mechanisms are not aligned to eliminating fatalities, enhancing capability, and minimising injury.	• The Defence Area has mechanisms in place to continually improve risk management, there are minor weaknesses, and the mechanisms are not aligned to eliminating fatalities, enhancing capability, and minimising injury.	• The Defence Area has effective mechanisms in place to continually improve risk management, and the mechanisms are aligned to eliminating fatalities, enhancing capability, and minimising injury.

Expectation 4.6 The Defence Area tracks changes, such as those impacting equipment, operations, infrastructure, training, people, plans and procedures, and takes action to manage associated risk.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence to demonstrate there is a process or system for risk assessing changes to equipment, operations, infrastructure, training, people, plans, and procedures.	• The Defence Area has a formal procedure for risk assessing changes to equipment, operations, infrastructure, training, people, plans, and procedures. There is some, but not enough evidence that these are consistently being reviewed by leadership and actions are being tracked to completion.	• The Defence Area has a formal procedure for risk assessing changes to equipment, operations, infrastructure, training, people, plans, and procedures that are reviewed by leadership. There is some but could be improved evidence that actions are not always tracked to completion.	• The Defence Area has a formal procedure for risk assessing changes to equipment, operations, infrastructure, training, people, plans, and procedures There is robust evidence that these are reviewed by leadership and actions are tracked to completion.

Expectation 4.7 A safety case is developed, maintained and reviewed where required to demonstrate that safety risks associated with complex systems and activities are being managed to a level that is ALARP and tolerable.

Unsatisfactory	Limited	Moderate	Substantial
• There is little or no evidence that the Defence Area identifies where safety cases are required. • There is little or no evidence that safety cases demonstrate that risks have been reduced to ALARP and are tolerable. • There is little or no evidence that safety cases are reviewed, maintained, or used to support safety decision-making. • Safety case findings are rarely or not communicated to relevant decision-makers and stakeholders.	• The Defence Area develops safety cases for some systems and activities where required, but this is not applied consistently. • Safety cases contain significant gaps in evidence, scope, or the demonstration that risks are ALARP and tolerable. • Safety cases are not routinely reviewed or updated to reflect changes to the system, activity, or operating environment. • Safety case findings are not consistently communicated to relevant decision-makers and stakeholders.	• The Defence Area develops safety cases for systems and activities requiring them and generally applies a proportionate approach. • Safety cases provide a structured argument supported by evidence that risks are being managed, although minor weaknesses remain in scope, evidence, or assurance arrangements. • Safety cases are reviewed and updated periodically, although records are not always readily accessible or fully current. • Safety case conclusions are generally communicated to relevant stakeholders and inform risk-based management decisions.	• The Defence Area systematically identifies where safety cases are required and develops them proportionately for all relevant systems and activities. • Safety cases provide a robust, evidence-based demonstration that risks have been reduced to ALARP and are tolerable. • Safety cases are regularly reviewed, maintained, and updated to reflect changes throughout the life of the system or activity and are readily accessible. • Safety cases actively support decision-making and governance and are consistently communicated which provides stakeholder confidence in the safe operation of the system or activity.