Ministry
of Defence

JSP 815 - Annex H

Audit Manual (Element 12)

Annex H - Audit Manual (Element 12)

JSP 815 Annex H (V1.1) September 2024

Contents

Title	Page
Safety assurance in Defence	2
Audit process	4
Linking safety system requirements and management arrangements	11
References	12
Appendix 1 - Example Letter to the Senior Officer / Chief Executive	1-1
Appendix 2 - Safety Management System Audit – Rating evaluation	2-1
Appendix 3 - Safety Management System – Rating categories	3-1

Amendment record

This Annex 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 of publication	Text affected	Authority
1.0	10 Sep 2024	New annex to support Element 12	DDS
1.1	20 Sep 2024	Update to convert Annex H into a writeable PDF	DDS

Safety Assurance in Defence

Introduction

1. Responsibility for management of safety is derived from the Secretary of State for Defence (SofS) Policy Statement. The amplification of the Statement is contained in Defence Policy for Safety that sets out the general Organisation and Arrangements (O&A) for Defence. The minimum necessary management arrangements for Safety are set out in JSP 815. It is however likely that audits will be combined to cover Environmental Protection, set out in JSP 816 and Fire set out in JSP 426. Defence organisations are to conduct assurance of their management arrangements including monitoring and review of governance, audit, and inspection in order to measure, correct, improve, and provide evidence about safety performance.

2. The evidence acquired from the assurance processes within a Defence organisation should principally be used to ensure compliance and enable continual improvement. Suitably summarised, it will support departmental safety performance reporting.

3. Assurance is carried out at three levels which starts with self-assurance by those directly responsible for delivering specific activities and then separately by those with oversight of management of the activity who are not responsible for delivery and finally by those that are totally independent of the Defence organisation. Independent assurance reviews (including audit or any other form of evaluation) are conducted on the safety management arrangements of organisations against the requirements of the SofS Policy Statement and subordinate pan-Defence safety policy. Such reviews may also be benchmarked directly against statutory or Defence regulatory requirements. These reviews provide an independent assessment for the organisation and support Defence in collating departmental reports to the most senior levels and in preparing the Defence Annual Assurance Report (AAR).

4. To help delineate the roles and responsibilities at the different levels of assurance Defence use the three Lines of Defence (LOD) approach. Some Defence organisations still refer to ‘parties of assurance’, however JSP 815 and this annex refers to LODs, the relationship between the two terms are as follows:

   a. 1st Party Assurance (1PA), which is the assurance undertaken by those responsible for delivering specific activities and equates to 1LOD assurance.

   b. 2nd Party Assurance (2PA), which is the assurance undertaken by specialists outside of the immediate chain of command but still within the Defence organisation and equates to 2LOD assurance.

   c. 3rd Party Assurance (3PA), which is the assurance undertaken by parties that are fully independent of the Defence organisation, generally by the DSA or the Government Internal Audit Agency (GIAA) and equates to 3LOD assurance.

Purpose

5. An audit is a significant part of an assurance process and is an essential tool used for checking that a Defence organisation’s safety processes are in place and are being followed. The purpose of an audit is to determine the level of adequacy and compliance against a set of agreed standards, policies, procedures, or requirements.

6. The Defence audit process is based on the ISO 19011 – Guideline for auditing management systems. The purpose of this annex to JSP 815 Element 12 is to provide guidance for Defence organisations on how to conduct safety audits as part of their 1 and 2 LOD assurance process.

7. Defence organisations have the freedom to use other audit methodologies appropriate to their business and activities that deliver the assurance requirements of Defence. As such, Defence organisations should compile evidence of compliance with those safety management arrangements specified in pan-Defence safety policy such as self-assurance and incident management. The link between this annex to Element 12 and provision of evidence to support Defence organisation performance reporting is further explored in Element 9.

Principles of audit

8. Auditing is characterised by reliance on a number of principles. These principles should help to make the audit an effective and reliable tool in support of management policies and controls, by providing information on which an organisation can act in order to improve its performance. Adherence to these principles enables auditors, working independently from one another, to reach similar conclusions in similar circumstances. The following are the main principles:

a. **Integrity** – to do the work with honesty, diligence, and responsibility.

b. **Fair presentation** – report truthfully and accurately.

c. **Due professional care** – able to make reasoned judgements in all audit situations.

d. **Confidentiality** – proper handling of sensitive or confidential information and ensure protection of the information.

e. **Independence** – auditor to be independent of the activity whenever possible and in all circumstances free from bias and conflict of interest.

f. **Evidence based approach** – evidence should be verifiable. It should be based on appropriate sampling of information available.

g. **Competence** – audit leads should have the necessary training, knowledge, skills, experience and behaviours (KSEB) to manage and conduct the audit. They should also have a good understanding of the audit principles, process and methodology.

Audit Process

9. An audit process should be based on the system requirements contained in documents and standards including; ISO45001[1], ISO14001, HSG 65, Defence policy, and provide evidence to inform Defence Key Performance Indicators (KPIs).

10. The role of safety auditors often includes an element of consultancy and post audit support, and the deliverables from the audit process include both formal debriefs to Safety policy areas and the communication of best practice across the department.

11. The key activities and roles to consider in the audit process include; ensuring the activity does not compromise the independence or objectivity of the audit function; the evidence and sample size necessary to support any finding; and whether any finding is likely to improve the organisation's risk management, control, and governance processes. Modern audits should endeavour to identify good practices as well as non-conformances.

Audit programme

12. An audit programme should be the first step in the audit process, planned over a set period of time, and based on a number of factors, including risk appetite, auditor and auditee availability, and possibly other factors like geography and climate to make sure that the timing of the audit works for all parties.

Plan the audit

13. Based on the audit programme, at approximately six months before the programmed audit start date, the nominated Audit Team Leader (ATL) is to inform the point of contact for the Defence organisation business area that is to be audited to confirm audit dates and to discuss and agree the objective, scope, and method of the audit. As a result of these discussions the ATL should produce a letter (example at Appendix 1) to formally notify the Head of the organisation of the intention to conduct the audit, the identified scope, and its proposed start date.

14. The ATL is to request access to relevant documents and records for planning the audit, scheduling the dates and also ask for any concerns or areas of interest in relation to the audit. They should determine who will be present to guide them and provide assistance required during the audit. The audit plan should be flexible enough to allow changes necessary as audit activities progress. The audit plan should cover the following, as appropriate: audit objectives, scope of the audit, audit criteria, location, expected time duration of the audit, audit team and their roles and responsibilities, follow-up actions from previous audit, follow-up activity after audit.

15. An annual audit programme of 3LOD assurance audits of Defence organisations, is submitted by the DSA to the DSEC for ratification and publication by the end of the preceding December. Further audits may be added to the programme throughout the audit cycle for example, in response to Service Inquiries, Incidents, or HSE / Environment Agency / SEPA intervention.

[1] ISO 45001 Occupational health and safety management systems

[2] BS EN ISO 14001 - Environmental Management Systems – Specifications with Guidance for Use.

[3] HSG65 - Successful Health and Safety Management.

16. The DSA conducts other forms of risk-based assurance including inspection, document review and permissioning roles which may also inform this governance.

17. Prior to undertaking any audit, a clear agreement is to be developed with the organisation to be audited. This agreement should include for example; citing the audit authority, audit scope and audit method, resources, timescales, outputs (normally a formal report), brief / debrief details, and sites to be visited.

Pre-audit meeting

18. For most safety audits, no later than three months before the audit commencement the ATL should arrange for an initial visit to take place. An exception to this arrangement would apply either when the Team Leader is sufficiently familiar with the organisation to be audited, or when the travel time / costs would mean that the visit would not be viable. In such a case planning for the audit should be made by correspondence, online meetings and telephone conversations.

19. The purpose of the initial visit is:

a. for the ATL to meet the point of contact within the Defence organisation’s safety team and may include anyone from the Defence organisation’s outer offices and the Head of the Safety Centre, the Establishment Safety Adviser / Officer (or equivalent) and to the Trade Union representatives as appropriate. This should provide the audit team with an understanding of the organisation's size, role, location and so on.

b. to agree the scope and intended outcomes of the audit.

c. to explain the method, purpose, and practice of the audit and the documentation required for review.

d. to agree an outline programme of dates, including a date for the ATL to call on the Head of the Unit / Organisation for a brief at the commencement of the audit. The outline programme should define areas to be visited and the personnel to be interviewed in the course of the audit, noting that the onus for arranging the programme for the audit rests with the organisation to be audited.

e. to meet focal points. Auditors normally require to be escorted for all their visits and for any tours they conduct. This is necessary to ensure both their safety and to make the greatest use of limited time by leading the way and making introductions to the personnel responsible for the areas they are visiting.

f. to discuss any specific safety risks which will be investigated in further detail during the audit.

20. The safety audit process is illustrated in Figure 1.

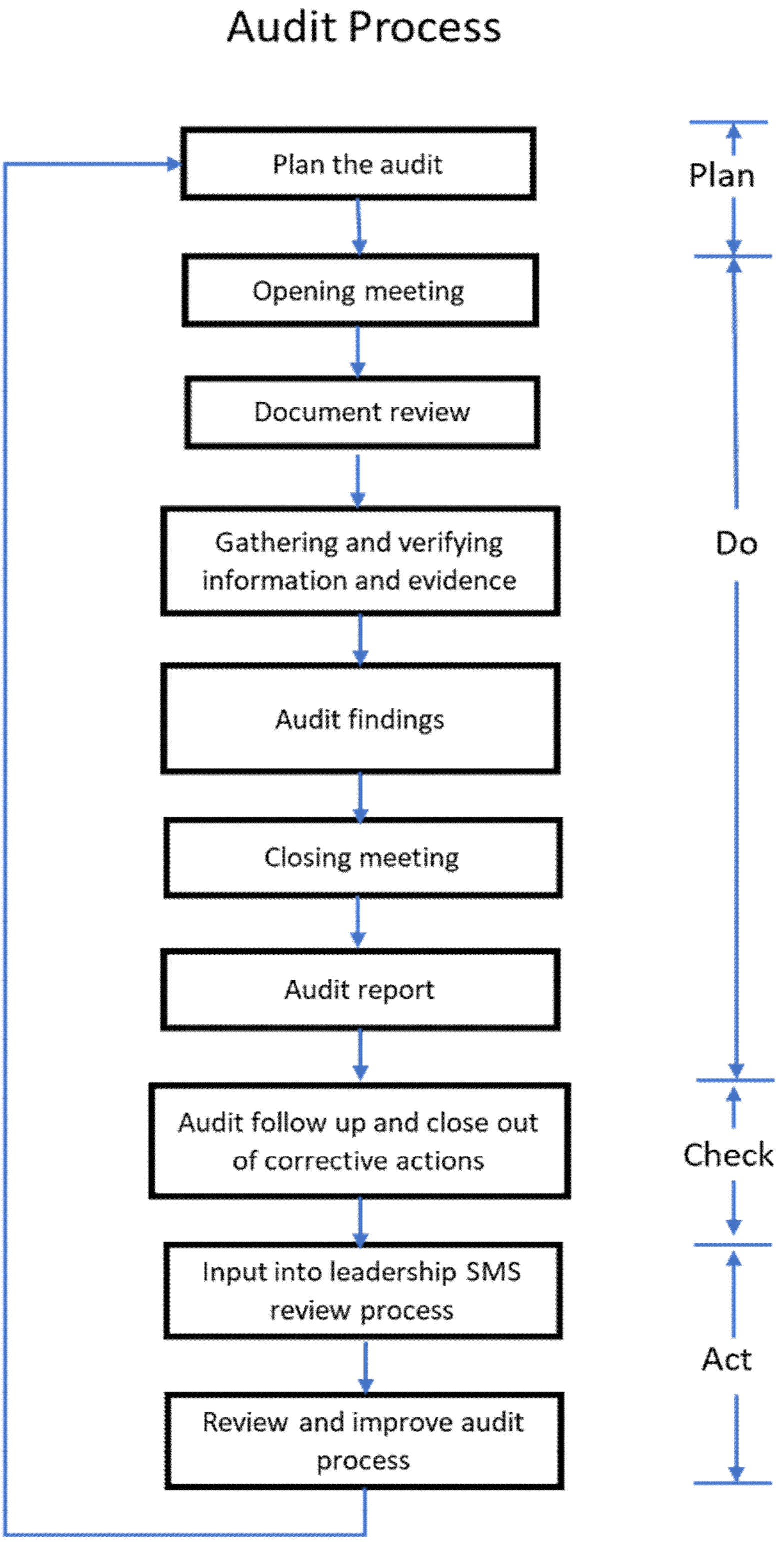
Audit Process
Plan the audit
Opening meeting
Document review
Gathering and verifying information and evidence
Audit findings
Closing meeting
Audit report
Audit follow up and close out of corrective actions
Input into leadership SMS review process
Review and improve audit process
Plan
Do
Check
Act

Figure 1 - Audit Process Map

Audit research

21. A safety management system (SMS) audit requires a detailed understanding of both the standard / policy under examination and the methods or processes used by the auditee to meet that standard or policy. Therefore, effective assurance by audit requires effort ahead of the field work, including review of documents and records applicable to the identified scope which should deliver focused interaction during that field work.

Document review

22. The document review can be done prior to or during the audit depending on the time, resources and complexity of the audit. The document review helps to determine the conformity of the system, against the audit criteria along with any evidence. Guidance about documents expected for each element is provided in the safety self-assessment toolkit Annex G. This is not an exhaustive list but can be used as a guide

23. An audit thread may expand the initial scope of an audit, by following a trail of evidence that reveals information about how health and safety is managed in the auditee's organisation. This is likely to also draw upon any corporate knowledge that the auditee may hold including findings of previous audits. A non-exhaustive list of the information sources which should be used in the pre-audit research is below:

a. Organisation and Arrangements (O&A) Statement, including who is responsible and accountable and how this is communicated to staff.

b. SMS documentation.

c. Safety assurance reports undertaken by internal or external bodies, including actions taken to close out recommendations.

d. impact assessments of any Suitably Qualified & Experienced Personnel (SQEP), SQEP shortfalls, and planned mitigation measures.

e. documentation from Boards or Committees set up to monitor / manage safety issues.

f. details of enforcement action (internal or external) and action taken as a result.

g. incident data, including fatalities, injuries and lessons learnt.

h. safety assurance and improvement plans. Risk control development plans.

i. annual safety reports.

j. Health and safety risk registers.

k. relevant agreements with other TLBs / EOs / Organisations on Safety issues.

Gathering and verifying information and evidence

24. Information relevant to the audit objectives, scope, and criteria, including information relating to interfaces between functions, activities, and processes, should be collected by means of appropriate sampling. Only information that is verifiable should be accepted as audit evidence. Audit evidence leading to audit findings should be recorded. If during the collection of evidence, the audit team becomes aware of any new or changed circumstances or risks, the team should address these accordingly.

Opening meeting (In-brief)

25. At the start of the audit, the ATL accompanied by the audit team should conduct an opening brief with the Head of the Organisation or an empowered representative. The briefing should include the following:

a. a brief summary of the scope, method, purpose, and practice of the audit.

b. discussion of the audit programme covering the areas to be visited.

c. an invitation to the Senior Officer / Executive to identify areas of concern, specific risks that need to be addressed, or good practices to be reviewed.

d. a description of the debrief procedure at the end of the audit and the Audit Report format and contents.

e. the option for a 'hot debrief' to be given to the Organisation's HS&EP Adviser and the Head of the Organisation as agreed at the end of the fieldwork phase.

Evaluation of management system requirements

26. Audits completed using the methodology in this volume should include an evaluation against the safety requirements of policy, legislation and applicable Defence regulation requirements as well as an assessment of the organisation's performance.

27. There may be occasions when it will be inappropriate for the evaluation to be completed, for example, when a safety management system is incomplete or under major change. In such cases the ATL should provide assistance to the development through a gap analysis and by making their services available for consultancy as required. Where an ATL is a Regulatory Inspector or appointed as an independent third party for services such as system certification their evaluation will be guided by an enforcement management model or certification criteria, as required.

Note: an incomplete or draft system would constitute a finding likely to require urgent action in order that the organisation can comply with Defence policy.

28. Safety management systems can be evaluated using a set of system requirements such as those in Appendix 2. These system requirements are fully supported by detailed safety system requirements as set out in JSP 815.

29. Auditors should complete the evaluation through a combination of interviews, review of documentation and site / process surveys. Interviewees should be selected based on the requirements of the scope being audited. For example, all staff could provide evidence of the effectiveness of the system to ensure adequate safety training, whereas evidence of management reviews may be taken from minutes of meetings. It is unlikely that one representative will be able to provide evidence of all safety system requirements.

Audit findings

30. Audit evidence should be evaluated against the Element 12 expectations to determine audit findings. Based on this and in line with the Government Internal Audit Agency (GIAA) assurance level categories, an assurance level of either (Unsatisfactory assurance, Limited assurance, Moderate assurance, or Substantial assurance) should be determined and also any non-compliance, opportunity for improvement and good practice to be identified.

31. When more than one auditor is involved, they should meet, discuss, and agree the audit findings prior to the closing meeting.

32. Auditors must keep a record of the evidence used for the evaluation noting details which decided the level of assurance; these should be recorded with the audit working papers at least until the next audit of that organisation.

Audit verification - evidence from site visits

33. The results gathered at the safety Rating Evaluation stage (Appendix 2) provide an indication of how the organisation’s SMS has been designed to function and if it is compliant with standards / policy as applicable to the scope. The next phase of an audit is to verify firstly that the systems are in use and secondly that in operation the management system is effective. It is therefore usual that auditors conduct a site visit verification procedure in order to confirm the standards being achieved.

Note: When visiting sites as part of an audit, the relevant Defence organisation leader or empowered representative or those responsible for the area or activity audited may request feedback on their safety performance. Whilst any immediate findings should be provided, it should be made clear that, in most cases, the audit scope is wider than the specific site, which is being used as part of the verification and evidence gathering process. It therefore may not be appropriate to share findings at this stage and the auditee sponsor should be consulted before sharing.

34. Auditors are to keep a record of their observations during the verification phase. These shall be retained with the audit working papers at least until the next audit of that organisation. These records may be useful at helping to work out the scope of the next audit or during audit follow-up meetings.

Closing meeting

35. The ATL should facilitate the closing meeting and present the audit findings for fact checking. The relevant Defence organisation leader or empowered representative, those responsible for the area or activity audited and the person responsible for safety should be invited to this meeting. For some audit situations the meeting may consist of communicating the audit findings while in other instances the meeting may be formal with minutes including a record of attendance that should be kept.

36. The closing meeting should include the audit evidence collected, based on the sample of information available and should present the audit findings in a way that is understood and acknowledged by the auditee. It should also include discussions on any corrective actions, complaints, or appeals.

Audit report

37. On completion of the audit, the Audit Report should be completed within the agreed timeframe discussed and agreed at the planning stage. The ATL should forward the report to the relevant Defence organisation leader or empowered representative, those responsible for the area or activity audited and the person responsible for safety. The report’s findings must be based on clear evidence and within scope to avoid any subsequent challenge.

38. Production of the Audit Report is the responsibility of the ATL. Each completed report should include the following elements:

a. an introduction that reiterates the scope, the audit team, and acknowledging the collaborative work with key personnel of the Defence organisation audited.

b. narratives addressing each of the 12 Element system requirements headings of JSP 815, with observations and recommended corrective actions which should form the basis of an Action Plan to be drawn up by the organisation auditee.

c. audit conclusions, including when the auditee should confirm acknowledgement of the audit findings and present a post-audit action plan to the ATL, which address the non-conformances raised during the audit.

d. annexes which could include Terms of Reference for the audit, the audit findings, a list of the organisations / places visited, a list of documents reviewed, progress made against recommendations from the previous audit, and any further evidence supporting the overall audit conclusions; this may include an evaluation of the organisation's performance against pre-determined standards, through the perspective of audit evidence for example: the completed Rating Evaluation (Appendix 2).

e. an Executive Summary, summarising the key conclusions, recommendations and observations of the audit.

39. The audit report template (safety self-assessment toolkit) is provided in Annex G. This template provides a scoring mechanism for each Element, as well as calculating an overall score covering all 12 Elements. Defence organisations can use this template and modify it to suit their needs if required or use an appropriate alternative template.

Issue report and debrief

40. Formal approval for issue of the Audit Report to the organisation under audit should be made by the auditing authority.

41. Whenever practicable, before releasing the Audit Report a formal debrief to the Head of the Organisation or an empowered representative of the audited organisation should be conducted by the ATL.

Audit follow-up actions

42. Following the formal debrief, the Defence organisation leader or empowered representative should be requested to produce an Action Plan based on the audit recommendations and observations. The priority and resources allocated to the Action Plan are the prerogative of individual budget holders. A copy of the organisation's Action Plan should be sent to the ATL in order for them to review it and make sure that it adequately covers the recommendations and observations raised in the audit report. If these are not considered to be acceptable then the ATL should contact the Defence organisation empowered representative under audit in order to agree an acceptable course of action.

43. A follow-up visit should be agreed, usually in six to nine months following the formal debrief, unless defined in the audit standard used. At the agreed time, the ATL should revisit the organisation to review implementation and progress against the agreed Action Plan.

44. The revisit should concentrate solely on issues raised within the audit report and should, where appropriate, include visiting the Head of the Organisation to discuss progress.

45. A post-visit letter should be drafted by the ATL to formally close the audit process. The letter should typically record:

a. the progress made against the action plan; and

b. the timing for the next review of actions or audit based on hazard profile and HS&EP management performance.

46. An update on issues raised during the audit, particularly any problems with policy implementation should be fed back into Defence organisation Leads for Safety and to the Director DS if appropriate, to ensure any necessary policy / procedural changes can be recommended to the policy / procedure owners.

Review and improve the audit programme

47. The Audit Programme Owner, if different to the ATL, should review the programme to assess whether its objectives have been achieved. Lessons learned from the audit programme review and audit findings should be used as inputs for continual improvement.

Input into leadership SMS review process

48. Overall performance improvement and actions identified in the audit should be included in the leadership review of the SMS. Defence organisations should review and report Audit outcomes as part of their Action Plan to respective senior leader(s).

Communication of good practice

49. Following each audit consideration should be made by both the auditor and auditee organisations to publish particularly effective and / or innovative safety management solutions encountered. The sharing of lessons learned from failings and also of good practice is considered an integral part of adding value to an organisation through the audit process. Promulgation should retain the anonymity of the organisation where possible.

Linking safety system requirements and management arrangements

Meeting statute and regulation

50. Defence organisations need to demonstrate how their SMS meets the requirements of the Secretary of State’s Policy Statement, and links with the specified elements of safety management arrangements and safety performance assessment levels applicable to their business and to the expectations of applicable statute and regulation.

51. Where appropriate, Defence organisations may use the Rating Evaluation system at Appendix 2 to assess their level of performance against twelve elements and expected performance levels as set out in JSP 815 or alternatively use audit report template (safety self-assessment toolkit) provided in Annex G.

52. In delivering this evaluation, it should be recognised that there is often no direct read across from one element to another. At best, there will be a reasonable degree of commonality but in one or two areas the link is dependent on the O&A and areas of responsibility.

53. Auditors will need to adopt a degree of common sense and judgement when measuring the outcomes of audits using this JSP 815 methodology to provide scores for the twelve elements. Other Performance Indicators and assessment methods are available and may be appropriate for a particular context. A Defence organisation should endeavour to record the means of their assessment particular to their own O&A in order that equivalence across multiple assessments may be maintained.

References

54. The following references are related to this annex.

a. Code of Practice for Independent Safety Assessors (ISA) - IET, SaRS, BCS, IMechE.

b. IOSH Code of Conduct.

c. IOSH Setting Standards in Health & Safety Advice - A Guide.

d. ISO 19011:2018 - Guidelines for Auditing Management Systems.

e. ISO/IEC 17000:2020 - Conformity Assessment.

f. Position Statement - The Institute of Internal Auditors - The Role of Internal Audit in Enterprise-wide Risk Management - Revised 2009.

g. Process Safety Performance Indicators and PSM Audit Programmes (IChemE).

h. The CQI and IRCA Professional Code of Conduct.

APPENDIX 1
TO ANNEX H

EXAMPLE LETTER TO THE SENIOR OFFICER / CHIEF EXECUTIVE

Audit of Safety Management Systems within [*Insert Organisation*]

In accordance with the overall audit programme required / agreed by [*insert authority*], I am proposing that an audit of [*insert organisation*] be undertaken during [*insert date*]. Initial contact and discussions with [*poc*] have indicated that this is viable.

The object of the audit is to assess compliance with the organisation's Safety Management System, in accordance with [*standard or reference*].

The audit team will be led by [*insert Name*] assisted by [*insert Name(s)*]. Arrangements should be made for the team to brief [*insert Name*], in order that they can explain the audit process used to assess compliance.

Following normal practice, the audit will be organised through [*insert details of organisation's Safety Representative*] and it would be helpful if you would give your authority for them to make available all relevant documentation and to organise any visits that the auditors require.

Where appropriate, contact should also be made for the auditors to meet a nominated Safety Representative from your Trade Union side, in order to explain the purpose of the audit.

Where appropriate good practices and non-conformances will be brought to your attention in the final report.

I hope you will find the audit useful in helping you to meet your management goals. Please do not hesitate to contact me if you have any queries.

APPENDIX 2
TO ANNEX H

SAFETY MANAGEMENT SYSTEM AUDIT – RATING EVALUATION

Organisation			**Lead Auditor**		
Interviewees					
Overall Rating		**Date of Audit**		**Signature**	

This Rating Evaluation and the Assurance Self-Assessment Toolkit at Annex G are examples of the many systems that may be used to provide an assessment of performance and enable Defence organisations to conduct 1LOD assurance and satisfy themselves that their Safety responsibilities are being met and are aligned to the Defence Safety Management System (SMS) Framework requirements (JSP 815). They also aim to support assurance activity in the 2LOD and 3LOD space and are both useful tools for Defence organisations to identify and share good practice. The use of this rating evaluation or the toolkit is not mandated by DDS.

Further guidance for verifying the System Requirements detailed in the Rating Evaluation is provided in Element 12.

Where an expectation requirement is not applicable to the organisation, it is to be deleted and the total possible Rating score reduced by 4 for the Section containing that requirement.

System Assurance Levels

1 - Applies to an UNSATISFACTORY ASSURANCE (Red) where there is evidence to demonstrate that the prescribed policies, processes and key controls are lacking or not well defined or **not actually embedded.** They **are not measured** to be able to assess **compliance** or are **not being adhered** to.

2 - Applies to a LIMITED ASSURANCE (Orange) where there is some but not enough evidence to demonstrate that the prescribed policies, processes, and key controls are operating and are fully embedded. They are **not actually operating as intended** or not operating in **numerous instances.**

3 - Applies to a MODERATE ASSURANCE (Yellow) where there is evidence to demonstrate that the prescribed policies, processes, and key controls that **should** be operating in your area are fully embedded **but these could be improved.** They are **actually** operating as intended but have identified some **minor areas known noncompliance.**

4 - Applies where a SUBSTANTIAL ASSURANCE (Green) where there is robust evidence to demonstrate that prescribed policies, processes, and key controls that **should** be operating in your area are fully embedded, are **actually** operating as intended and **no weaknesses** have been identified.

N/A (Grey) – Indicates that there is **‘No information yet available’** or is **‘Not applicable’** to the Defence organisation or out of scope.

Element 1: Leadership, Governance and Culture

Elements of safety management arrangements	Rating	Evidence of process and/or implementation
System requirement		
This element focuses on the extent to which a Defence organisation has a vision, clear aims, and objectives about what it can and wants to achieve in terms of safety. Together with effective leadership, governance methods promote a consistent approach to safety management at all levels and support a positive, proactive culture of reporting and learning. This is supported by establishing accountability based on well-defined authority levels, acceptance of decision-making and a clear understanding of responsibilities.		
E1.1 To what extent Leadership set the "tone from the top" and actively demonstrate their commitment to safety?		
E1.2 To what extent does Leadership promote a culture of continual improvement, speaking up and embedding transparent and open reporting?		
E1.3 How well does Leadership set clear safety responsibilities by which the Defence organisation is measured and held to account?		
E1.4 To what extent are Leadership visible at all levels of the Defence organisation; including through direct interactions with the wider workforce and other stakeholders on matters of safety?		
E1.5 How well does corporate governance hold safety as an equal partner to other strategic objectives such as capability, cost, and schedule?		
E1.6 To what extent is there a culture is in place which fosters resilient safety management, engages people, and promotes effective safety behaviours?		
Sub Total:		

Element 2: Organisation and Dependencies

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
This focus of this element requires that the Defence organisation's structure facilitates and encourages flexibility and collaborative working, while managing the associated safety risks and dependencies. This includes: a. Intra-organisation working between Defence organisations, with teams that are formed to best meet delivery requirements and mitigate safety risks rather than aligned with organisational boundaries; b. Inter-organisational working, such as with other government departments and the supply chain, which brings in experience and expertise from external parties; and c. Clear understanding on dependencies and appropriate delegations are in place across internal and external boundaries.		
E2.1 How well does the Defence organisation develop and maintain an SMS that is specific to their area of responsibility. How well does it set out how the Defence SMS Framework and underpinning policy and regulations will be delivered in a way specific to the Defence organisation?		
E2.2 How well does the Defence organisation define its safety roles, responsibilities, and accountabilities in its SMS?		
E2.3 How well does the Defence organisation demonstrate that it has a system in place to allocate appropriate resources (i.e. budget and people)?		
E2.4 How well does the Defence organisation demonstrate that it has arrangements in place to share information about safety risks, supporting effective risk management and continual improvement?		
E2.5 To what extent do the Defence organisation check that the standards of safety management of its contractors and suppliers meet or exceed Defence standards?		

E2.6 How well does the Defence organisation demonstrate it has mechanisms for joint consultation with the workforce, contractors, and supply chain in place?		
E2.7 How well does the Defence organisation demonstrate that changes to their organisational structure or changes to personnel with specific knowledge or experience are evaluated, risk assessed, approved, and documented?		
E2.8 To what extent are there mechanisms in place to identify functional and organisational dependencies and interfaces, and how safety risks are managed across these?		
Sub Total:		

Element 3: Legislation, Policy, Regulations and Guidance

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
This focus of this element requires that the Defence organisation identifies and communicates the requirements of legislation, policy and guidance surrounding safety. Leadership sets out how safety contributes to the organisation's success and achievement of objectives and puts in place a framework for making balanced decisions at all levels both within the organisation and across other Defence organisations.		
E3.1 How well does the Defence organisation demonstrate that it has mechanisms in place to identify and maintain compliance with safety Legislation?		
E3.2 How well does the Defence organisation demonstrate that it has mechanisms in place to comply with all relevant Defence safety expectations?		
E3.3 How well does the Defence organisation demonstrate that their policy and guidance is consistent and does not conflict with the Defence SMS Framework?		
E3.4 To what extent does the Defence organisation have mechanisms in place to communicate with internal and external stakeholders the requirement to comply with safety legislation, Defence policy and guidance and Defence regulations?		
E3.5 How well does the Defence organisation ensure policies and guidance are reviewed regularly to reflect any significant changes?		
E3.6 How well does the Defence organisation demonstrate that it has a process in place to manage exemptions from statute, and exemptions / waivers / concessions from Defence regulation?		
Sub Total:		

Element 4: Risk Assessment and Safety Cases

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
This focus of this element requires that the Defence organisation 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.		
E4.1 To what extent does the Defence organisation have mechanisms in place to assess its risk profile and identify its safety hazards?		
E4.2 To what extent does the Defence organisation have in place to manage its safety risks, including provision of proportionate controls?		
E4.3 How well does the Defence organisation demonstrate where safety risks are significant, these risks are elevated, and leadership are actively involved in their management?		
E4.4 How well does the Defence organisation demonstrate it has arrangements in place to communicate safety risk to all stakeholders, outlining control measures needed to provide safe working practices?		
E4.5 How well does the Defence organisation demonstrate it has mechanisms in place to continually improve risk management with the aim of eliminating fatalities whilst enhancing Defence capability and minimising injury?		
E4.6 How well does the Defence organisation demonstrate it tracks changes, such as those impacting equipment, operations, infrastructure, training, people, plans and procedures, and takes action to manage associated risk?		

E4.7 How well does the Defence organisation demonstrate that a safety case is maintained throughout the acquisition lifecycle that identifies, evaluates, and manages the risk from concept development through to disposal?		
Sub Total:		

Element 5: Supervision, Contracting and Control Activities

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
This focus of this element requires that the Defence organisation has implemented safe systems of work to control activities and meet its legal duty of care requirements. It has arrangements for application of these systems that includes supervision of all the workforce and contractors. Leadership has effective frameworks in place to ensure that they have sufficient and timely oversight of the Defence organisation and its supply chain using the four Cs: coordination, co-operation, communication, and control. This should also apply to Duty Holding where there is a credible and reasonably foreseeable Risk to Life (RtL) and where other statutory arrangements are seen to be inadequate.		
E5.1 How well does the Defence organisation demonstrate it has mechanisms in place to delegate authority for the control of activity?		
E5.2 How effective are the arrangements for ensuring that those holding delegation of authority are trained and competent to discharge their responsibilities?		
E5.3 How well does the Defence organisation demonstrate that 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?		
E5.4 How well does the Defence organisation demonstrate that those with delegated authority are formally appointed via a letter of delegation?		

E5.5 How well does the Defence organisation demonstrate that those responsible for the control of activity have a duty to mitigate risk to As Low As Reasonably Practicable (ALARP) and tolerable?		
E5.6 How well does the Defence organisation demonstrate that those responsible for control of activity have the authority to pause or cease activity where a risk is no longer ALARP and tolerable?		
E5.7 How well does the Defence organisation demonstrate that it has developed and implemented Safe Systems of Work (SSW), to safeguard those carrying out the work or affected by it?		
Sub Total:		

Element 6: Personnel Competences, Resources and Training

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
The focus of this element requires that the Defence organisation has identified all roles with safety responsibilities and have in place a means of identifying skills, knowledge, experience, behaviours, and expertise requirements of those roles. Where this is not met by the existing workforce, plans are developed to address and mitigate gaps through workforce planning, formal and informal training, and development. Sufficient resources and funding are identified to maintain competence and ensure continual professional development.		
E6.1 How well does the Defence organisation demonstrate it has sufficient resources in place aligned to its risk profile?		
E6.2 How well has the Defence organisation defined responsibilities, accountabilities and delegations for safety management?		
E6.3 How well does the Defence organisation demonstrate it has plans in place to support recruitment, deployment, career development, retention and succession of its people?		
E6.4 How well does the Defence organisation demonstrate that training programmes are in place that include safety skills enabling the workforce to meet Defence requirements?		
E6.5 How well does the Defence organisation demonstrate that a competency process is in place to assess and assure qualifications, behaviours, skills of the workforce to meet Defence safety requirements?		
Sub Total:		

Element 7: Equipment Design, Manufacture and Maintenance

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
The focus of this element requires that the Defence organisation has put in place frameworks and working practices to incorporate safety considerations into the design, acquisition, manufacture, operation, modification, and maintenance of equipment, including Defence digital systems.		
E7.1 How well does the Defence organisation demonstrate that it has mechanisms in place to identify and assess safety risks and requirements associated with equipment throughout its entire lifecycle; from Concept, Assessment, Demonstration, Manufacture, In-service and Disposal (CADMID)?		
E7.2 To what extent does the Defence organisation have mechanisms in place to ensure risks associated with equipment are adequately controlled and mitigated through its entire lifecycle and where necessary elevated to the appropriate Duty Holder, SRO, and competent person?		
E7.3 To what extent does the Defence organisation have mechanisms in place to ensure equipment is compliant with statute and Defence regulation throughout its lifecycle. Where necessary, an exemption / waiver / concession is in place where compliance is not achievable?		
E7.4 How well does the Defence organisation demonstrate that it has processes in place to ensure equipment is always maintained and operated within defined design and operating limits. Mechanisms are in place to communicate these operating limits to those who operate and maintain equipment?		

E7.5 How well does the Defence organisation demonstrate that it has mechanisms in place to ensure physical changes to equipment (including major software changes), materials and associated specifications are evaluated, risk assessed, approved, and documented?		
E7.6 How well does the Defence organisation demonstrate that it has mechanisms to accurately identify and manage the safety risks and dependencies in their equipment supply chain?		
E7.7 How well does the Defence organisation demonstrate that lessons learned from previous equipment design, acquisition, manufacture, operation, modification, and maintenance activities are shared effectively across the Defence organisation?		
E7.8 How well does the Defence organisation demonstrate that it has mechanisms in place to assess the risk from integration of equipment and systems and its effects on platform safety?		
Sub Total:		

Element 8: Infrastructure Design, Build and Maintenance

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
The focus of this element requires that the Defence organisation has put in place frameworks and working practices to incorporate safety considerations into the strategic and technical design, spatial coordination, acquisition, manufacture and construction, handover, use, modification, maintenance, and disposal of infrastructure.		
E8.1 How well does the Defence organisation demonstrate that it has mechanisms in place to identify and assess safety risks and requirements associated with infrastructure throughout its entire lifecycle; from Concept, Assessment, Design, Manufacture and Construction, Use, Maintenance, and Disposal?		
E8.2 How well does the Defence organisation demonstrate that it has mechanisms in place to ensure risks associated with infrastructure are adequately controlled and mitigated through its entire lifecycle and where necessary elevated to the appropriate Duty Holder, SRO, Head of Establishment, and competent person?		
E8.3 How well does the Defence organisation demonstrate that it has mechanisms in place to ensure infrastructure is compliant with statute and Defence regulation throughout its lifecycle. Where necessary, an exemption / waiver / concession is in place where compliance is not achievable?		
E8.4 How effective are the Defence organisation processes that are in place to ensure infrastructure is maintained and operated within its intended use. Mechanisms are in place to communicate these processes to the workforce that operate and maintain the infrastructure?		

E8.5 How well does the Defence organisation demonstrate that it has mechanisms in place to ensure physical changes to infrastructure, (including major software changes), materials and associated specifications are evaluated, risk assessed, approved, and documented?		
E8.6 How well does the Defence organisation demonstrate that it has mechanisms to accurately identify and manage the safety risks and dependencies in its infrastructure supply chain?		
E8.7 How effective are lessons learned from previous infrastructure design, acquisition, build, operation, modification, and maintenance activities are shared effectively across the Defence organisation?		
Sub Total:		

Element 9: Performance, Management Information and Reporting

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
This element focuses on the extent to which the Defence organisation has put in place the mechanisms to generate and communicate complete and accurate Management Information on a timely basis. There are methods in place to define data requirements, and then collect, record, manage and report on its safety performance, including incidents, accidents, and good practice.		
E9.1 How well does the Defence organisation demonstrate it has effective systems and processes in place to collect, measure and monitor safety performance, using documented leading, lagging, and cultural performance indicators?		
E9.2 How well does the Defence organisation demonstrate that it regularly reviews performance and conducts trend analysis to inform decisions and implement plans to correct performance deficits?		
E9.3 How well does the Defence organisation demonstrate it has effective mechanisms in place to produce, report and review the management information from performance indicators and trend analysis; acting on it in a timely manner?		
E9.4 How well does the Defence organisation demonstrate that leadership decisions around cost, schedule and military capability performance are data driven, including assessment of potential safety impact?		
Sub Total:		

Element 10: Accident / Incident Management and Emergency Response

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
The focus of this element requires that the Defence organisation has frameworks in place to report, notify, record, investigate incidents and plan on how to address investigation recommendations. The Defence organisation should promote an environment in which there is a culture of learning, where all our people and those external to the organisation feel safe to report incidents. Lessons are identified and learnt through a process of continual improvement. There is a proactive approach to identifying and mitigating potential incidents through regular and effective creation and testing of emergency plans.		
E10.1 To what extent does the Defence organisation promote a culture of open reporting of mistakes, accidents, incidents and near misses that occur?		
E10.2 To what extent has the Organisation put a system in place which is consistent with the Defence policy to record and report incidents, accidents and near misses from initial submission to close-out, allowing for effective investigation and resolution?		
E10.3 How well does the Defence organisation demonstrate that it has resources in place to investigate incidents, accidents and near misses?		
E10.4 How well does the Defence organisation demonstrate that it has systems in place to implement the corrective actions and learning from incidents, accidents and near misses to manage and drive continual improvement?		
E10.5 To what extent are emergency and business continuity plans put in place, tested regularly, and consider safety matters?		
Sub Total:		

Element 11: Communications and Stakeholder Engagement

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
The focus of this element requires that the Defence organisation has mechanisms in place to identify its internal and external stakeholders and communicate and engage with these stakeholders on safety matters.		
E11.1 How well does the Defence organisation demonstrate it has mechanisms in place to identify internal and external stakeholders and understand their role and purpose in safety matters?		
E11.2 How well does the Defence organisation demonstrate it has mechanisms in place to manage and engage with stakeholders and to consult on safety matters, including with the workforce, trade unions, suppliers, contractors, and others affected by the organisation’s activities?		
E11.3 How effective is the Defence organisation’s work with its stakeholders to build effective working relations to drive continual improvement in safety?		
E11.4 How well does the Defence organisation demonstrate it has mechanisms in place to allow all people, contractors, and the supply chain to easily access up to date safety information relevant to their roles?		
E11.5 How well does the Defence organisation demonstrate it has mechanisms in place to enable people to anonymously raise safety related concerns?		
Sub Total:		

Element 12: Assurance

Elements of safety management arrangements	Rating	Evidence of process and / or implementation
System requirement		
The focus of this element requires that the Defence organisation has assurance mechanisms in place to identify strengths and weaknesses in its SMS and it drives continual improvement. Assurance activity is planned to cover all business activities and is linked to having a risk-based assurance plan.		
E12.1 How well does the Defence organisation demonstrate it has mechanisms in place to conduct a risk-based 1st Line of Defence (1LOD) assurance appropriate to its scale and complexity?		
E12.2 How well does the Defence organisation demonstrate it has mechanisms in place to conduct 2LOD assurance and has mechanisms in place to enable 3LOD assurance and support external assurance?		
E12.3 How effectively does the Defence organisation conduct an annual self-assessment against the elements of the Defence SMS Framework and provide this to organisational leadership to identify opportunities for improvement and help inform the generation of the annual assurance report submission?		
E12.4 How effectively does the Defence organisation's leadership formally review the effectiveness of their SMS in meeting organisational objectives based on assurance activity undertaken?		
E12.5 How well does the Defence organisation demonstrate it has mechanisms in place to ensure that corrective action is taken to address Defence and statutory regulator enforcement actions?		
Sub Total:		

SAFETY MANAGEMENT SYSTEM ASSURANCE RATING

	Rating (1 to 4 per category)	
	Awarded	**Possible**
a. Element 1 - Leadership, Governance and Culture		24
b. Element 2 - Organisation and Dependencies		32
c. Element 3 - Legislation, Policy, Regulations and Guidance		24
d. Element 4 - Risk Assessment and Safety Cases		28
e. Element 5 - Supervision, Contracting and Control of Activities		28
f. Element 6 - Personnel, Competence, Resources and Training		20
g. Element 7 - Equipment Design, Manufacture and Maintenance		32
h. Element 8 - Infrastructure Design, Build and Maintenance		28
i. Element 9 - Performance, Management Information and Reporting		16
j. Element 10 - Accident / Incident Management and Emergency Response		20
k. Element 11 - Communications and Stakeholder Engagement		20
l. Element 12 - Assurance		20
TOTAL		**292**
OVERALL SMS ASSURANCE RATING		**100%**

APPENDIX 3
TO ANNEX H

SMS ASSURANCE RATING CATEGORIES

Assurance level	Comments
Substantial **95 - 100%**	You have robust evidence to demonstrate that prescribed policies, processes, and key controls that **should** be operating in your area **are fully embedded**. You have robust evidence to demonstrate that policies, processes and key controls **actually** help you manage your key risks. You have robust evidence to demonstrate that the policies, processes and key controls are **actually** operating as intended and no weaknesses have been identified.
Moderate **75 - 94%**	You have evidence to demonstrate that prescribed policies, processes and key controls that **should** be operating in your area are fully embedded **but these could be improved**. You have evidence to demonstrate that these policies, processes and key controls **actually** help you manage your key risks. You have evidence to demonstrate that the policies, processes and key controls are **actually** operating as intended, but have identified some **minor areas known noncompliance** with the defined policies, processes and key controls.
Limited **50 - 74%**	You have **some, but not enough** that prescribed policies, processes and key controls are operating and are embedded. You **do not have confidence** that the policies, processes and key controls are designed to **actually** help you manage your key risks. You have evidence to demonstrate that the policies, processes and key controls are **not actually operating as intended** or not operating in **numerous instances.**
Unsatisfactory **Below 50%**	You have evidence that the prescribed policies, processes and key controls are **lacking or not well defined** or **not actually embedded**. You have evidence that the policies, processes and key controls are defined, but as designed, **do not** help you manage your key risks. You have evidence that the policies, processes and key controls **are not measured** to be able to assess **compliance or** are **not being adhered** to**.**