Ministry of Defence

JSP 815 Volume 2

Element 12: Assurance

JSP 815 Volume 2 Element 12 (V1.1) June 2023

Contents

Amendment record

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

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

Terms and definitions

General safety terms and definitions are provided in the Master Terms and Definitions Glossary which can also be accessed via the GOV.UK page. The HMT Orange Book – Management of Risk – Principles and Concepts defines assurance as:

“A general term for the confidence that can be derived from objective examination of information over the successful conduct of activities, the efficient and effective design and operation of internal control, compliance with internal and external requirements, and the production of insightful and credible information to support decision-making. Confidence diminishes when there are uncertainties around the integrity of information, or of underlying processes.”

Must and should

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

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

Scope

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

Introduction

1. This element provides the direction that must be followed and the guidance and good practice that should be followed which will assist users to comply with the expectations for assurance that are set out in Element 12 of Volume 1 to JSP 815 (this JSP).

2. Responsibility for the management of health, safety, and environmental protection (HS&EP) is derived from the Secretary of State for Defence's (SofS) Policy Statement. The SofS Policy Statement sets out the commitment and role of the Defence organisations senior leaders to ensure that safety policies and regulations are applied throughout Defence and that their Defence activities are delivered in line with the Defence Safety Management Systems (SMS) and their own Defence organisation's SMS.

3. The amplification of the SofS Policy Statement is contained in Defence policy for HS&EP which also sets out the general Organisation and Arrangements (O&A) for Defence to manage HS&EP. The minimum necessary management arrangements for safety policy are laid out in JSP 815. The management arrangements for environmental protection policy are laid out in JSP 816.

Purpose and expectations

4. This element is to assist the Defence organisation to put in place assurance mechanisms to identify strengths and weaknesses in its SMS and drive continual improvement. Assurance activity should be planned to cover all business activities and linked to a risk-based assurance plan.

5. Defence organisations have the freedom to use audit methodologies that are appropriate to their business and activities, however they must provide evidence of compliance with safety legislation, Defence policy and regulation.

General assurance process

6. Assurance is about providing adequate confidence and evidence, through due process, that safety requirements have been met. It is also about monitoring performance and checking how well risks are being controlled. It is less about assurance as a 'tick box exercise' and more about identifying problems and providing objective information to decision makers so remedial action can be taken. Health and Safety Executive guidance (HSG) 65 provides additional advice to those who need to put in place or oversee their organisation's health and safety arrangements.

Risk-based approach

7. A risk-based approach means focussing assurance effort on the activities and controls which give rise to the most significant safety risks that may impact upon the successful delivery of the Defence organisation’s objectives. It can also include focussing assurance in areas where the most benefit will be derived from the effort. This means a high-level prioritisation approach to identifying, assessing, reporting, and assuring the effectiveness of an organisation’s safety management.

Assurance methods

8. A Defence organisation’s assurance process should provide an objective examination of evidence providing an independent, objective assessment of risk management, and control or governance processes.

9. There are a range of assurance methods that can be used to provide confidence in safety management. Below are some examples of different assurance methods. More detail can be found in ISO 19011[1].

Oversight / surveillance

10. Oversight involves monitoring safety performance, verifying that activities comply with policies and reviewing processes and documents. Surveillance can be undertaken by observing work performed.

Workplace inspection

11. On-site safety inspections can measure the management of safety at a workplace level and help identify if improvements are needed. An inspection can help to identify hazards or processes that are not working efficiently.

12. In addition, inspections can be used to confirm the safe condition of equipment or workplaces. For example, the Provision and Use of Work Equipment Regulations 1998 (PUWER) states the requirement to inspect workplace equipment. This ensures that equipment is maintained, safe to operate and any deterioration can be detected and corrected in good time. Compliance checks on firefighting equipment or first aid kits would also be an example of a focused workplace inspection.

Safety visits

13. The opportunity for the Defence organisation’s management to explore the effectiveness of risk control measures through planned visits to workplaces to observe tasks and discuss controls. Opportunity for the management to show commitment to safety and communicate with personnel.

[1] ISO 19011 Annex B describes Interviews, checklists, questionnaires, document reviews, sampling, observations etc as potential aspects of Audits.

Sampling

14. Sampling is the selection of a representative amount or group of items, people, and areas, which are examined to establish compliance and used to indicate the standard of compliance for the wider group. Sampling is required when it is not practical or cost effective to examine all available information e.g., records are too numerous or too dispersed geographically to justify the examination of every item.

Surveys

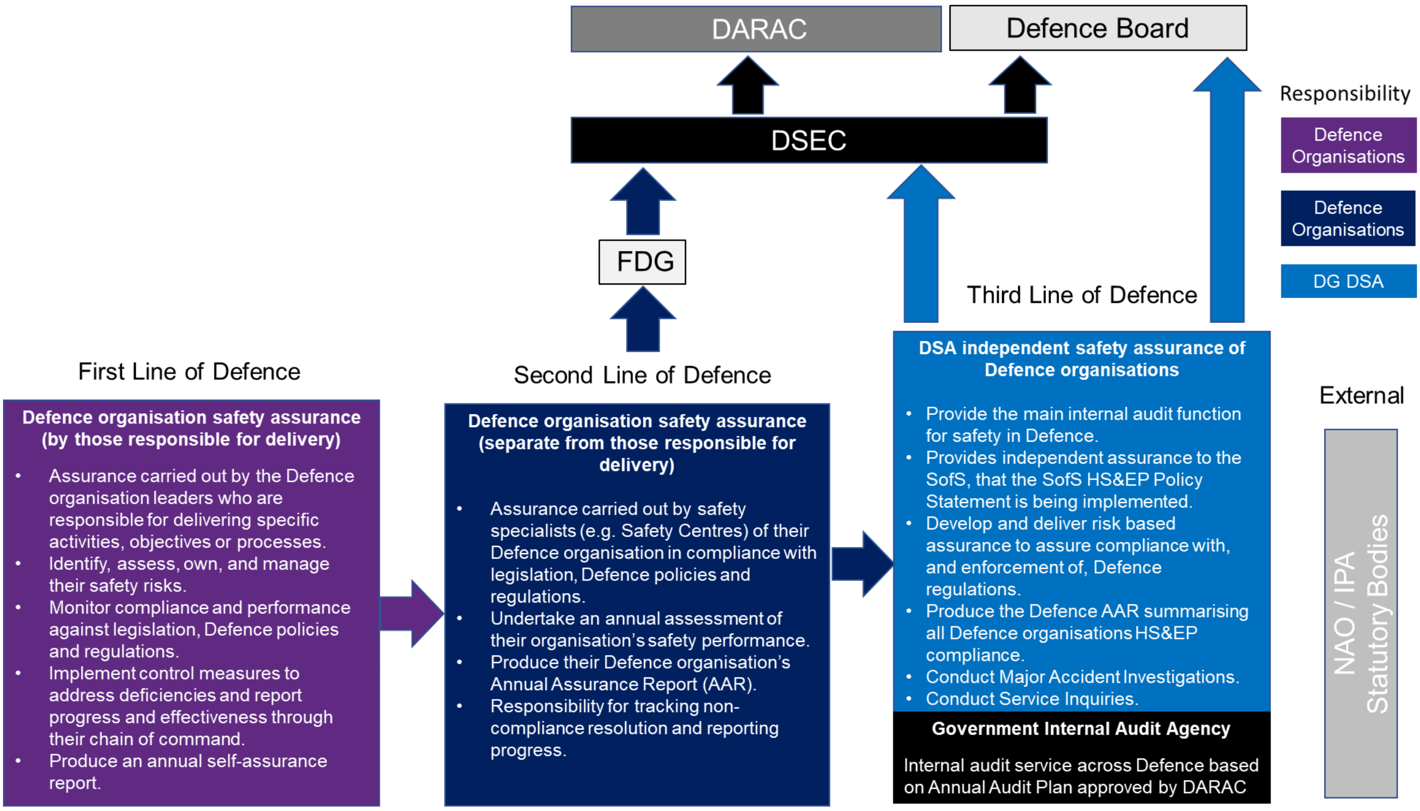
15. Surveys are where a set of questions (computer or paper based) are asked of a targeted audience to gain a general view from that audience on a given topic. A safety cultural survey would be an example of this.

Audits

16. The purpose of an audit is to determine the level of adequacy and compliance against a set of agreed standards, policies, procedures, or requirements. In safety, the minimum standard may be derived from legislation, Defence policy and regulation. An SMS audit looks at the compliance towards components of a Defence organisation's safety management system with the audit criteria based on the Defence SMS requirements and Defence policy.

Three Lines of Defence model

17. To better understand who is responsible for what assurance activity, Defence use the three Lines of Defence (LOD) approach for ease of delineating roles and responsibilities. The three LOD for safety is depicted in Figure 1.



Defence organisation safety assurance (by those responsible for delivery)

- Assurance carried out by the Defence organisation leaders who are responsible for delivering specific activities, objectives or processes.
- Identify, assess, own, and manage their safety risks.
- Monitor compliance and performance against legislation, Defence policies and regulations.
- Implement control measures to address deficiencies and report progress and effectiveness through their chain of command.
- Produce an annual self-assurance report.

Defence organisation safety assurance (separate from those responsible for delivery)

- Assurance carried out by safety specialists (e.g. Safety Centres) of their Defence organisation in compliance with legislation, Defence policies and regulations.
- Undertake an annual assessment of their organisation's safety performance.
- Produce their Defence organisation's Annual Assurance Report (AAR).
- Responsibility for tracking non-compliance resolution and reporting progress.

DSA independent safety assurance of Defence organisations

- Provide the main internal audit function for safety in Defence.
- Provides independent assurance to the SofS, that the SofS HS&EP Policy Statement is being implemented.
- Develop and deliver risk based assurance to assure compliance with, and enforcement of, Defence regulations.
- Produce the Defence AAR summarising all Defence organisations HS&EP compliance.
- Conduct Major Accident Investigations.
- Conduct Service Inquiries.

Government Internal Audit Agency

Internal audit service across Defence based on Annual Audit Plan approved by DARAC

Figure 1: Three Lines of Defence

First Line of Defence (1LOD)

18. 1LOD assurance comes directly from those responsible for delivering specific activities, objectives or processes. It may lack independence, but its value comes from those who know the business, culture and day-to-day challenges. Assurance must be provided by those responsible for delivering the activity (normally at unit, estate, establishment or platform level) and can be aligned to the DDH. The 1LOD needs to be focussed on building the confidence (through evidence) that Defence safety policy and regulation is understood and being followed.

19. The 1LOD within the Defence organisation is to identify, assess, own, and manage their safety risks. The Defence organisation is therefore responsible for designing, implementing, and maintaining their own control measures, monitoring their adherence, and implementing corrective actions to address deficiencies.

20. Defence organisations provide an annual self-assurance report at 1LOD to their Safety Centre (or equivalent) which then informs the 2LOD Annual Assurance Report (AAR).

21. At the most fundamental level it is about leaders continually asking the question “how do I know” the activity within their area of responsibility is safe to proceed? The “how do I know” question places the emphasis on the leaders to check, test and understand the safety risks associated with the activities for which they are responsible.

22. Leaders are responsible for ensuring that their Defence organisation design, operate and improve their policies and processes to provide compliance and performance against legislation, Defence policies and regulations. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight ineffective control measures. Where possible this should be supported by relevant and timely management information.

23. Defence organisations can tailor their internal assurance arrangements (1LOD). However, they must have adequate processes in place to provide self-assurance at the unit, estate, establishment or platform level. They should also retain evidence of compliance and show how this delivers against the standards set in JSP 815 Volume 1.

24. Where remedial activity is required, the 1LOD should implement control measures to address deficiencies and report the progress and the effectiveness of the control measures up through the Defence organisation’s chain of command (CoC).

Second Line of Defence (2LOD)

25. 2LOD assurance is the oversight of management of activity, separate from those responsible for delivery but not independent of the Defence organisation’s management chain. The 2LOD assurance must be provided by the CoC, separate from the assurance given by those responsible for delivering the activity and in line with formal Military Command or Defence organisation assurance mechanisms. This assurance may be achieved within the Defence organisation by those that are specialised in safety management and assurance such as the Safety Centres or Chief Environment and Safety Officer (CESO) teams or equivalent.

26. The Defence organisation’s 2LOD should have a defined and proportionate approach, so that the methodology for assurance is applied effectively and appropriately. Defence organisations must undertake assessment of 1LOD to provide assurance that their organisation is compliant (understood and being followed) with legislation, Defence policies and regulations.

27. The safety professionals in the Safety Centres and CESO (or equivalent) team must undertake an annual assessment of their organisation and lead in the production of an Annual Assurance Report (AAR) of their organisation’s safety performance against the Defence Safety Management System (SMS) Framework as detailed in JSP 815 Vol 1.

28. To assist in the Defence organisation’s self-assessment, a safety self-assessment toolkit has been created at Annex G (the use of this self-assessment is not mandatory, but if used this would satisfy the minimum assessment standard required to provide assurance against JSP 815).

29. Safety Centres or the CESO team (or equivalent) are responsible for tracking the non-compliance resolution and agreeing the close out of actions. The Safety Centres (or equivalent) are responsible for reporting the progress and close out of corrective actions (through the Performance and Risk Reviews (P&RR)).

Third Line of Defence (3LOD)

30. 3LOD consists of any organisation that provides an “internal audit” capability. Through its independence, an internal audit function will provide an objective evaluation of how effectively an organisation assesses and manages its risks. It includes an evaluation of the design and effectiveness of the operation of the “first and second lines of defence.” It often does so through a risk-based approach, by evaluating all elements of the risk management framework and risk and control activities. An effective and holistic internal audit function delivered by many organisations, may also enhance the assurance picture of the management of cross-organisational risks, thereby supporting the sharing of good practice between organisations.

Defence Safety Authority (DSA)

31. For safety in Defence, the DSA provides the main internal audit function within 3LOD. It provides independent assurance to the Secretary of State (SofS) and the Department that the Secretary of State’s policy on HS&EP is being implemented in the conduct of Defence activities. This is achieved through proportional and appropriate evidence-based assessment activity. It is empowered through its Charter, on behalf of the SofS for Defence, for its roles as the independent regulator, investigator and assurer for HS&EP within Defence. To maintain the DSA’s independence, the Director General takes their authority from the DSA Charter.

32. The DSA is responsible for:

a. providing independent assurance to the Secretary of State and the Department that the SofS Policy Statement on HS&EP in Defence is being implemented in the conduct of Defence activities. This will be achieved through proportional and appropriate regulatory and evidence-based assessment activity.

b. preparing an Annual Assurance Report including a summary of HS&EP compliance and risk for consideration by the Second Permanent Secretary, the Defence Board, and onward consideration by the Secretary of State.

c. ensuring that, within each regulatory area, Defence Regulators plan and conduct their own risk-based assurance activity, maintain, promulgate, assure compliance with, and when necessary, enforce Defence regulations; and to promote an engaged HS&EP culture.

d. ensuring that there is an effective appeals process to review enforcement action if it is challenged by those to whom it applies, to include escalation through the relevant chain of command, up to Secretary of State if necessary.

e. ensuring that all HS&EP related fatalities, serious injuries, significant environmental incidents and major capability loss are appropriately investigated to identify lessons, make recommendations, promote continuous improvement, and minimise the risk of reoccurrence.

f. ensuring that, in any circumstances where the Director General judges HS&EP concerns are not being satisfactorily addressed through normal Departmental processes, they retain the right of direct access to the Secretary of State to raise those concerns, while ensuring that the Second Permanent Secretary is kept informed.

Government Internal Audit Agency (GIAA)

33. The GIAA Internal Auditing service for Defence will report to Defences Accounting Officer providing assurance to the Permanent Secretary (PS) and the Defence Audit, Risk and Assurance Committee (DARAC); a subcommittee of the Defence Board. Internal Audit is a key part of the Department's assurance framework and in many ways is unique due to its scope across the whole department.

34. The GIAA provide an independent third line (3LOD) assurance function and its role is to provide independent and objective assurance, advice and insight over the risk management, governance and internal control processes within Defence.

35. With the exception of Military Operations, all business systems, processes, functions and activities within Defence may be subject to internal audit work. The GIAA Defence annual risk-based audit plan defines what activities will be reviewed by them and is formally approved by the DARAC. Further information on the GIAA can be found at Government Internal Audit Agency (Formally Defence Internal Audit) (sharepoint.com).

External assurance

36. External Assurance bodies are outside the immediate Department boundary, but they are part of the risk management framework. Defence organisations should work closely with these groups and provide timely information and access when requested.

37. External assurance is provided by:

a. independent regulatory and inspection bodies (e.g., HSE);

b. external system accreditation reviews / certification (e.g., International Organisation for Standardisation (ISO));

c. HM Treasury / Cabinet Office / who support and review approval processes;

d. the Infrastructure and Projects Authority (IPA), who provide independent expert assurance reviews of major government projects including business case appraisal and consideration of H&S risks; and

e. external auditors, chiefly the National Audit Office (NAO), who have a statutory responsibility for financial statements and risk management impact including to safety.

38. Defence organisations should also familiarise themselves with the Memorandums of Understanding (MOU) between the MoD and HSE, other Statutory Regulators and devolved HSE agency in Northern Ireland. When dealing with these bodies the Defence organisations may wish to consult their legal department for further advice and guidance.

Total assurance

39. Assurance is about providing confidence that safety policy and regulations are embedded and being followed across the Defence organisations; risks are identified and managed; and assurance activities identify learning opportunities to support continual improvement.

40. Total assurance is about the holistic picture and confidence derived from separate assurance activities at all LOD levels and culminates in the Defence AAR collated by the DSA. The Defence AAR is a product of the DSA's information cohering and provides an independent assessment of how the Department is doing with regards to implementing Defence's HS&EP policies and regulations in order to provide the Department with a benchmark against which to measure progress, understand trends and identify issues that need to be addressed. The findings from the DSA AAR are reported to the Defence Board, DARAC, and DSEC.

41. Total assurance is not the expectation that assurance will cover all activities equally and with the same depth of review. It brings together risk and assurance in a joint approach to provide confidence in:

a. the successful conduct of activities or SMS integration into wider Corporate Governance;

b. the efficient and effective design and operation of internal control;

c. compliance with internal and external statutory and policy requirements;

d. the production of insightful and credible information to support organisational governance and decision-making; and

e. The risk-based approach allows for targeted activity, making best use of limited resource where it is most needed and minimising the regulatory burden on Defence organisations.

Audit process

42. This audit process is based on the ISO 19011 – Guideline for auditing management systems. The Defence organisations need to demonstrate how their SMS meet the requirements of the SofS Policy Statement and aligns with the Defence SMS Framework (JSP 815 Volume 1). JSP 815 Volume 1 aligns with ISO 45001. A useful comparison between these two can be found in Annex F.

43. The role of a safety auditor can include an element of advisory and post audit support. The deliverables from the audit process include both formal debriefs to safety policy areas and the communication of good practice across the Defense organisation. The key activities and roles to consider 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. Audits should endeavor to identify good practices as well as non-compliance.

Principles of audit

44. 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 competence (the skills knowledge and experience) to manage and conduct the audit. Auditors should have knowledge about audit principles, procedures, methodology.

45. Within Defence, a safety auditor should also be familiar with this JSP 815 Element 12 and JSP 815 Volume 1, and their Defence organisation's activity, processes, and safety risks. Auditor competence can also affect confidence in the audit process and ability to achieve its objectives.

46. The audit will consist of the top-level elements in Fig 2 but the order can be tailored to suit the circumstances of the audit.

Plan the audit

47. Based on the audit programme, the nominated audit lead is to inform the point of contact within the Defence organisation regarding the planned audit to discuss and agree the objective, scope, and method of the audit.

48. The audit lead is to request access to relevant documents and records for planning the audit and 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.

Opening meeting

49. The audit lead accompanied by the audit team, should conduct an opening meeting with the relevant Defence organisation leader or empowered representative. During the meeting, an opportunity to ask questions should be provided. Depending on the safety audit scope and complexity the opening meeting may simply consist of communicating to the auditee that an audit is being conducted and explaining the nature of the audit. The degree of detail should be consistent with the familiarity of the auditee with the audit process.

50. The purpose of the opening meeting is to confirm the agreement of all parties (e.g., auditee, audit team) to the audit plan (unless already agreed beforehand), introduce the audit team and ensure that all planned audit activities can be performed.

51. The opening meeting should include the following:

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

b. discussion of the audit plan covering the areas to be visited. This also includes who will be interviewed as a part of the audit.

c. an invitation to the relevant Defence organisation leader or empowered representative 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 (or another pre-determined time period) and the audit report format and contents.

Document review

52. The document review can be done prior to the audit 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 JSP 815 Vol 1 at the beginning of each element and in the safety self-assessment toolkit Annex G. This is not an exhaustive list but can be used as a guide.

Gathering and verifying information and evidence

53. 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.

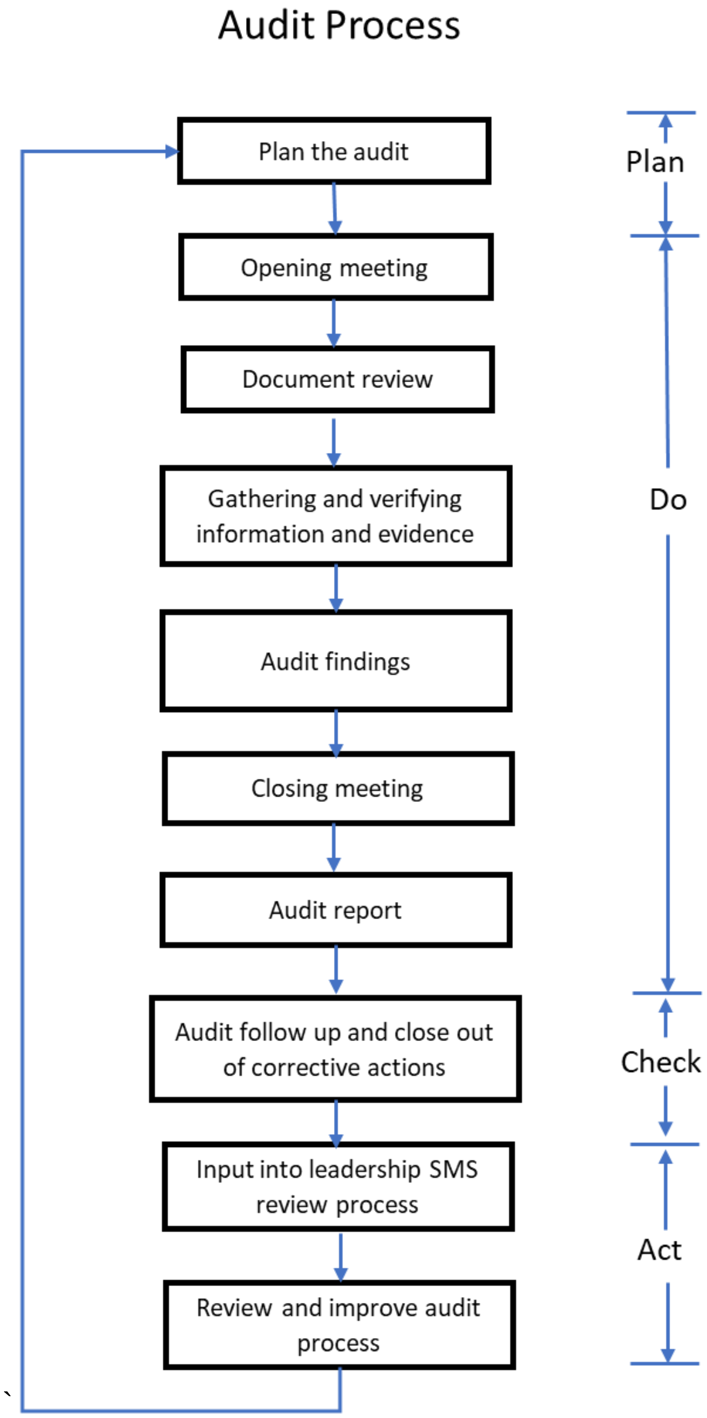

Audit Process
Plan the audit
Opening meeting
Document review
Gathering and verifying information and evidence
Audit findings
Closing meeting
Audit report
Audit follow up and close out of corrective actions
Input into leadership SMS review process
Review and improve audit process
Plan
Do
Check
Act

Figure 2: Audit Process

Audit findings

54. Audit evidence should be evaluated against the JSP 815 Volume 1 expectations to determine audit findings. Based on this, an assurance level (No assurance, Limited assurance, Substantial assurance, and Full assurance) should be determined and also any non-compliance, opportunity for improvement and good practice to be identified. When more than one auditor is involved, they should meet, discuss, and agree the audit findings prior to the closing meeting.

55. Auditors will need to adopt a degree of pragmatism and judgement when measuring the outcomes of audits using this JSP 815 methodology to provide scores for the 12 Elements. Other performance indicators (PIs) and assessment methods are available and may be appropriate for a particular context. A Defence organisation should endeavor to record the means of their assessment particular to their own O&A in order that equivalence across multiple assessments may be maintained.

Closing meeting

56. The Audit lead 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.

57. 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

58. On completion of the audit, the Audit Report should be completed within the agreed timeframe discussed and agreed at the planning stage. The audit lead 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.

59. Production of the Audit Report is the responsibility of the audit lead. Each completed report should include the following elements:

a. an Executive Summary.

b. narratives addressing non-compliance, observation related to each element of the Defence SMS (JSP 815 Volume 1).

c. audit conclusions.

d. a recommendation which should form the basis of a subsequent action plan. The action plan is to be generated by the auditee.

e. annexes which could include Terms of Reference for the audit, the audit findings, a list of the Defence 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 Defence organisation's performance against pre-determined standards, through the perspective of audit evidence.

60. The audit report template (safety self-assessment toolkit) that covers the Defence SMS (JSP 815 Volume 1) audit is provided in Annex G. This template also 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.

Audit follow up and close out of corrective actions

61. Following the issue of the audit report the empowered representative should be requested to produce an Action Plan based on the audit findings. The empowered representative is to allocate the necessary resources to produce and implement the Action Plan. A copy of the Action Plan should be sent to the audit lead in order for them to review the plan 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 audit lead should contact the Defence organisation empowered representative under audit to agree an acceptable course of action.

Review and improve the audit programme

62. The Audit Programme Owner, if different to the Audit Lead, 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

63. 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).

Sharing good practice

64. Following each audit, consideration should be made by the Defence organisation to share (internally and / or with other Defence organisations) effective and / or innovative safety management solutions encountered as a result of the audit. The sharing of lessons learned from good practice where further improvement is required is an integral part of adding value to a Defence organisation through the audit process. Promulgation should retain the anonymity of the Defence organisation where possible.

Element summary

65. The Defence organisation senior leadership should ensure that their organisation:

a. has mechanisms in place to conduct a risk-based 1LOD assurance appropriate to its scale and complexity.

b. has mechanisms in place to enable 2LOD and 3LOD assurance, including external assurance.

c. conducts an annual self-assessment against the elements of the Defence SMS and provides this to the organisational leadership to identify opportunities for improvement and help inform the generation of the annual assurance report submission.

d. formally review the effectiveness of their SMS in meeting organisational objectives based on assurance activity undertaken.

e. has mechanisms in place to ensure that corrective action is taken to address Defence and statutory regulator enforcement actions.