

# 35 Safety and the management of change

This chapter is split into two parts:

**Part 1: Directive.** This part provides direction that you **must** follow to help you comply with (keep to) health and safety law, Defence policy and Government policy.

**Part 2: Guidance.** This part provides the guidance and good practice that **should** be followed and will help you to keep to this policy.

## Contents

Title	Page
Amendment record	1
Terms and definitions	2
Scope	2
Assurance	2
<b>Part 1: Directive</b>	
Introduction	3
Management of change policy statements	4
Other change management responsibilities	9
<b>Part 2: Guidance</b>	
Organisational Safety Assessments - Process guidance	10
Training	18
Retention of records	18
Related documents	18
<b>Annexes</b>	
Annex A – Six phases of the OSA flow chart	A1

## Amendment record

This chapter 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](mailto:COO-DDS-GroupMailbox@mod.gov.uk).

Version No	Date of publication	Text affected	Authority
1.2	Oct 20	Interim update post-handover of policy from DSA to Dir HS&EP.	Dir HS&EP
1.3	21 Sep 23	Release of two-part chapter structure and additional OSA process guidance.	DDS
1.4	10 Oct 2023	Amendments to Policy Statement 2, including the addition of other procurement methods.	DDS

## Terms and definitions

The following table sets out definitions of some of the key terms used in this chapter. The general safety terms and definitions are provided in the [Master Glossary of Safety Terms and Definitions](#) which can also be accessed via the [GOV.UK](#) page.

Accountable person	The person whose terms of reference state that they are responsible for making sure there are suitable and sufficient systems in place to control health and safety risks in their unit, estate (site) or platform. This term is used in place of CO, HoE, OC, Station Commander and so on, or as decreed by the Defence organisations.
Equipment	The term 'equipment' in this chapter refers to all types of equipment, vehicles, platforms, systems or services that are acquired to meet a capability / requirement.
Change owner	The change owner is the person who initiates, and has overall accountability for the safe implementation of, the change project / programme.
Occupational stress	Occupational stress is the negative psychological and physical effects an employee experiences due to the responsibilities, environment, or other pressures of the workplace.
Organisational Safety Assessment (OSA)	An Organisational Safety Assessment (OSA) is a process to manage organisational change and assess the proposed Organisation and Arrangements (O&A) compared with those that were in place prior to that change. The OSA is a logical, phased evaluation of the impact of the organisational change on safety and includes the identification of any potential safety risks and the mitigation or control measures required to manage those safety risks to ALARP and tolerable.
Senior Responsible Owner (SRO)	The Senior Responsible Owner (SRO) is the formally appointed individual with overall accountability for ensuring that a project / programme is governed effectively, meets its objectives and delivers the projected benefits.
User	The User is the Defence organisation who has taken ownership, and has been nominated as the lead organisation, for that equipment and is responsible and accountable for the equipment to be 'operated safely'.

### Must and should

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

Where this chapter 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).

### Assurance

The application of this policy **must** be assured (that is, its use **must** be guaranteed). As part of their overall assurance activity, the commander, manager or accountable person (AP) **must** make sure that this policy is followed and put into practice effectively. Assurance **must** be carried out in accordance with JSP 815 Element 12.

# Part 1: Directive

## Introduction

1. The effective management of change **must** include the identification of any potential hazards that a change can introduce, then assessing the risks and the impact on safety associated with these hazards and addressing them in a systematic way.
2. Any change to equipment, infrastructure, policy or to the organisation could introduce risk and unintended or unsuspected consequences. Therefore, a formal and systematic process **must** be used to manage any change from conception through to implementation to identify potential safety hazards and managing their risks.
3. The systematic process to manage any change **should** follow the 'Plan, Do, Check, Act' approach<sup>1</sup>. This **should** start at the planning stage **before** the change has been fully developed, continued and monitored **during** the change process and reviewed **after** it has been implemented.
4. The systematic approach applied to all changes to equipment, infrastructure, policy or to the organisation **must** include evaluation, risk assessment, approval, implementation and documentation. The system applied **should** always be **proportional** to the complexity and the scale of the change but **must** include the following essential elements:
  - a. agree and evaluate the justification for the change at the appropriate management level;
  - b. risk assess the proposed change using a multi-disciplinary team of competent people, including specialists, contractors, vendors and suppliers when their particular, knowledge, skills, experience, behaviours (KSEB) is required;
  - c. consider the findings of the risk assessment when deciding whether or how to go ahead with the change;
  - d. put in place a rigorous design approval system to make sure that the appropriate standards are applied to the design. Any deviations from the design are to be approved by a competent suitably qualified and experienced person (SQEP) with sufficient KSEB;
  - e. write formal procedures to implement the change, train all personnel who are directly affected by the change and obtain confirmation that training has been effective;
  - f. confirm the change has been communicated to all stakeholders; and
  - g. implement the change, monitor and review the assumptions after an agreed period and confirm mitigations remain valid.

---

<sup>1</sup> For more information on the Plan, Do, Check, Act approach (see [HSE guidance note HSG 65](#)).

## Management of change policy statements

5. Defence has established the following policy statements, which **must** be followed:

a. **Policy Statement 1.** All physical changes to a facility, building or infrastructure (including software changes and amendments to specifications) **must** be proportionately; evaluated, risk assessed, approved, implemented and documented.

b. **Policy Statement 2.** All physical changes to equipment (including software changes, modifications and amendments to specifications) **must** be proportionately; evaluated, risk assessed, approved, implemented and documented.

For projects, programmes and other procurement methods, where a risk assessment is not sufficient to demonstrate that the safety risks associated with that equipment have been adequately identified, communicated and/or controlled, then a safety case **must** be developed.

c. **Policy Statement 3.** All changes to, or deviations from, requirements in a regulation, policy or training provided by or on behalf of Defence **must** be proportionately; evaluated, risk assessed, approved, implemented and documented.

d. **Policy Statement 4.** All changes to an organisational structure or change in personnel with specific knowledge, skills, experience, behaviours (KSEB) **must** be assessed to understand the impact of the organisational change on safety. Where proportional to do so the change owner **must** decide whether an Organisational Safety Assessment (OSA) needs to be conducted.

e. **Policy Statement 5.** At the concept of any change initiatives set out in Policy Statements 1 to 4, the change owner **must** identify and appoint a suitable Senior Responsible Owner (SRO).

### Policy Statement 1

All physical changes to a facility, building or infrastructure (including software changes and amendments to specifications) **must** be proportionately; evaluated, risk assessed, approved, implemented and documented.

6. This policy applies to **all** physical changes to any facility or building including changes to the infrastructure or its use and software changes to IT systems.

7. This policy is applicable to **all** physical changes throughout the lifecycle of a facility or building from design, construction, commissioning, operation, and decommissioning. The framework for the operation of the Defence estate is set out in the [Infrastructure Operating Model \(IOM\)](#), Infrastructure Control Framework and [JSP 850 Infrastructure and Estate Policy](#).

8. Prior to implementing the physical changes to a facility or building, the Senior Responsible Owner **must** ensure a pre-start up safety review is conducted to:

a. make sure that all actions from the risk assessment process have been incorporated into the design and any deviations from established standards or practices have been approved at the appropriate level;

- b. make sure that the Construction (Design & Management) Regulations 2015 are complied with and that engagement with the relevant MOD Licensing Authority takes place where applicable;
- c. confirm that all necessary safety checks and tests have been successfully completed after the change (for example any electrical or fire alarm checks and tests);
- d. confirm that procedures for operating the facility or building are in place and personnel are trained in the use of these procedures; and
- e. confirm the change has been communicated to all stakeholders.

9. The Senior Responsible Owner **must** ensure that continuous monitoring and safety reviews be conducted throughout the change implementation phase.

10. Once the physical changes to a facility or building have been completed, these changes **should** be monitored closely by personnel with sufficient KSEB. Feedback and lessons learned **should** be recorded for the benefit of continuous improvement and future projects.

### **Policy Statement 2**

All physical changes to equipment (including software changes, modifications and amendments to specifications) **must** be proportionately; evaluated, risk assessed, approved, implemented and documented.

For projects, programmes and other procurement methods, where a risk assessment is not sufficient to demonstrate that the safety risks associated with that equipment have been adequately identified, communicated and/or controlled, then a safety case **must** be developed.

11. This policy is applicable to all physical changes to any equipment including changes to the equipment software systems and includes changes to how the equipment is operated or changes to the environment in which it is operated if they are outside of those for which it was designed or commissioned. This policy is applicable throughout the lifecycle of an equipment from design to commissioning, operation, and decommissioning.

12. Prior to implementing the physical changes to any equipment, as part of the governing arrangements a modification and design review **must** be conducted by a competent (SQEP) or by personnel with sufficient KSEB to:

- a. make sure that all actions from the risk assessment process have been incorporated into the design and any deviations from established standards or practices have been approved at the appropriate level;
- b. confirm that all necessary testing has been successfully completed;
- c. confirm that procedures for operating the equipment are in place and personnel are trained in the use of these procedures; and
- d. confirm the change has been communicated to all stakeholders.

13. Once the physical changes to the equipment have been completed, these changes **must** be monitored closely by personnel with sufficient KSEB. Feedback and lessons learned **should** be recorded for the benefit of continuous improvement and future projects.

14. Where a risk assessment is not sufficient to demonstrate that the risks to the equipment have been adequately identified, communicated and/or controlled, then a safety case **must** be developed. A safety case is used to provide compelling evidence that equipment is safe for a given application in a given operating environment. A safety case **must** capture all the safety related risks associated with that equipment and evidence how these risks will be managed to as low as is reasonably practicable (ALARP) and to a tolerable level.

15. The Senior Responsible Owner (SRO) or the User, is responsible for making sure that a safety case has been produced and that all relevant safety issues have been considered. Safety cases are covered in JSP 815 Part 2 (Elements 4 and 7) and in more detail in JSP 376 - Defence Acquisition Safety Policy.

### **Policy Statement 3**

All changes to, or deviations from, requirements in a regulation, policy or training provided by or on behalf of Defence **must** be proportionately; evaluated, risk assessed, approved, implemented and documented.

16. This policy is applicable to all changes to, or deviations from, requirements in a regulation, policy or to training provided by or on behalf of Defence. The safety implications of such changes **must** be considered by the change owner by following a systematic process to make sure that the change is evaluated, risk assessed, approved, implemented and documented.

17. Where changes or amendments are made to Defence regulations, policy or other controlled documents then a record of those amendments and the reasons for them **must** be maintained by the change owner.

18. Where deviations from requirements are necessary or Defence organisations are unable to comply with all or parts of JSP 375 Defence safety policy, they **must** notify the Director of Defence Safety with the specific details of why they are permanently unable to comply with all or parts of that safety policy.

19. Where deviations from or changes to a document have been completed, these **should** be monitored closely by personnel with sufficient KSEB. Feedback and lessons learned **should** be recorded for the benefit of continuous improvement.

20. Where design changes have been identified to training courses that are provided by or on behalf of Defence, the changes **should** be reviewed and verified by the Training Requirements Authority (TRA) and relevant stakeholders updating the Training Authorising Document (TrAD) which is then to be formally endorsed (usually at a Customer Executive Board (CEB)) in accordance with Defence Systems Approach to Training (DSAT) set out in JPS 822. Without the TrAD being endorsed the delivery of training cannot commence. Once the change to training has been endorsed and implemented, the safety of those delivering and those receiving the training **must** be considered by the course owners, the Training Delivery Authority (TDA) and an appropriate risk assessment **must** be carried out in accordance with the Safe System of Training covered in JSP 375 Chapter 8 (Safety Risk Assessment and Safe Systems of Work).

#### Policy Statement 4

All changes to an organisational structure or change in personnel with specific knowledge, skills, experience, behaviours (KSEB) **must** be assessed to understand the impact of the organisational change on safety. Where proportional to do so the change owner **must** decide whether an Organisational Safety Assessment (OSA) needs to be conducted.

21. Organisational change encompasses any changes affecting the structure or range of duties currently conducted by personnel within that organisation and may include mergers, organisational restructuring, transfers of Defence personnel or changes to staffing levels and alterations to procedures, roles and responsibilities.

22. Any organisational change has the potential to introduce safety hazards and risks and therefore all changes to an organisational structure or change in personnel with specific KSEB **must** be assessed to understand the impact of the organisational change on safety.

23. The Secretary of State (SofS) HS&EP Policy Statement says; 'Any senior leader of a Defence organisation proposing organisational change where there is potential for significant impact on safety or environmental standards and performance is to ensure that, before being implemented, the impacts of the proposed change are properly assessed through an Organisational Safety Assessment (OSA) to demonstrate that any detriment to these standards and performance are mitigated to be ALARP and tolerable'.

24. An OSA is a formal and systematic process that is used to assess the proposed Organisation and Arrangements (O&A) compared with those in place prior to the organisational change and identify any potential safety risks and the required mitigation measures to manage those risks to ALARP and tolerable. The OSA is a logical, phased evaluation of the impact of the organisational change on safety from the conception through to implementation of the change and is used to ensure that there is no adverse impact to the safe conduct of Defence activities resulting directly or indirectly from the change.

25. When organisational change occurs the change owner **must** decide whether an OSA needs to be conducted. It is for the change owner to determine the appropriate authority and relevant competency required. If additional guidance is required then the change owner **should** consult with their Chief Environment and Safety Officer (CESO) or equivalent or the nominated Safety Centre OSA point of contact. The change owner **must** make an initial assessment of the change and decide if an OSA is required, if so then the scale of the OSA **should** be proportionate to the complexity and scale of the proposed change and **must** be conducted by a person in a position of authority, with suitable KSEB to conduct such an assessment. Further guidance on conducting OSAs is covered in Part 2 of this chapter.

### Policy Statement 5

At the concept of any change initiatives set out in Policy Statements 1 to 4, the change owner **must** identify and appoint a suitable Senior Responsible Owner (SRO).

26. The change owner is the initiator or sponsor of any change programme, it may be the Defence organisation senior leader, the Chief Executive of an Agency or another government organisation or it may be the Head of Business Area depending on the level at which the change is being driven.

27. The change owner **must** identify and appoint a Senior Responsible Owner (SRO) or equivalent<sup>2</sup>, who has the appropriate authority, relevant competency and who would normally have responsibility for all safety issues associated with that change. The SRO appointment does not mean the safety team / advisors should be automatically appointed.

28. The SRO **must** be identified and appointed as early into a change initiative as possible, normally at the conceptual stage. The SRO is responsible for making sure that the application and scope of this policy is proportionate to the complexity and scale of the proposed change. They are also responsible for co-ordinating and collating all the risk assessments, contingency plans, and hazard operability studies for the area(s) affected by the proposed change in conjunction with the appropriate management and personnel.

29. Depending on the scale of the change the SRO **should** compile an Implementation Plan for the change owner and this plan **must** be reviewed at regular intervals. The Implementation Plan **should** contain the individual action plans and key performance indicators, together with continuity plans to cover those roles with safety responsibilities requiring specific competences and the tasks that personnel in those roles carry out, contractors **should** also be involved in this process.

30. Where an Implementation Plan has been compiled, the SRO **must** make sure that it is communicated effectively along with any associated processes to all those involved in or affected by the change. The SRO **should** also co-ordinate the effective and frequent cascade of information between all levels of management and personnel and ensure that feedback of concerns from all levels is supported and encouraged (personnel **should** be provided with feedback following receipt of their comments).

31. At the earliest stage of the change process the SRO **must** consider the involvement of all stakeholders including military and civilian personnel, contractors and Trade Unions (where appropriate) and representatives of the relevant organisation safety teams. The change process **must** be conducted in an open and transparent manner with clear accountability for decisions.

---

<sup>2</sup> In some circumstances, when proportionate, the change owner may also be the SRO.

## Other change management responsibilities

### Accountable person (AP)

32. The accountable person (AP) in the context of this chapter, is responsible for managing the safety risks associated with changes to facilities, buildings, infrastructure, equipment, policies and organisational changes within their area of responsibility. In some cases, the AP may be the change owner or the SRO. If they are the change owner, they may decide to delegate the SRO role.

33. Prior to the implementation of change the AP **must** make sure that a review is undertaken to confirm the existing baseline or establish one and the fitness for purpose of the existing safety management system. The review **should** determine the potential impact on the existing arrangements for managing safety, and the interim and long-term control measures required to mitigate any potential adverse effects of the proposed change; for example, organisational structure, staffing levels, staff disposition, roles and responsibilities or any other change that may directly or indirectly affect the control of the hazard.

### Commanders and managers

34. Commanders and managers are responsible for making sure that risk assessments (covered in JSP 375 Volume 1 Chapter 8) are reviewed as part of the change process, and that any additional risk assessments identified are completed and the results discussed with the SRO. Risk assessments, including those for the period of transition **must** be reviewed regularly (at least once every 6 months until the organisation matures and confidence in the systems and control measures can be validated). Where occupational stress assessments have been undertaken commanders and managers **must** make sure that they are regularly reviewed to identify any areas of concern to personnel, for example where there is a threat of redundancy, outsourcing, move of location, or low morale. Commanders and managers **should** encourage feedback from their personnel which **should** be fed back up to the SRO.

35. During the change process commanders and managers **must** review activities under their control for any indications of overload on systems or personnel from the change, for example near-misses that have resulted from the change, or any delays, backlogs or excessive working hours. Commanders and managers **should** develop a fallback plan which includes stopping the change if the changes show signs of increasing risks to safety. This may require advising the change owner / SRO that certain activities **must** cease until control systems are put in place to reduce the risks.

### Individuals

36. All individuals have a responsibility to follow the relevant policy and direction communicated to them on the process of change management. Personnel **must** complete any training requirements identified and provided as part of change management and report any safety concerns resulting from the change.

37. Personnel **should** raise any concerns with their commander or manager if they feel that changes may have, or are having, an impact on their own or another person's safety. Personnel may also wish to discuss their concerns with workplace Trade Union or Employee Safety Representatives.

## Part 2: Guidance

This part provides the guidance and good practice that **should** be followed and will help you to keep to this policy.

### Organisational Safety Assessments - Process guidance

1. The following Organisational Safety Assessment (OSA) process guidance aims to:
  - a. Describe the requirement, roles and responsibilities for assessing organisational change impact on safety risks managed within an organisation;
  - b. To provide guidance on responsibilities for safety during any transformation;  
and
  - c. To define the content and process for conducting and assuring an OSA.

### Background

2. Change is an inevitable part of business improvement at all levels in an organisation, from increasing the efficiency of a process or updating equipment, to making major changes to organisational staffing and structure. However, while the impacts of simple changes can be readily assessed to demonstrate their effectiveness, those at the organisational level can be more difficult because of the complexity involved or the lack of recognition of the potential impact on standards of safety.

3. The evidence for this comes from investigations<sup>3</sup> into significant safety accidents across the world. The Haddon-Cave Review following the loss of Nimrod (XV230) observed that, “MOD suffered a period of deep organisational trauma between 1998 and 2006 due to the imposition of unending cuts and change which led to the dilution of its safety and airworthiness regime and culture...”. It is for these well understood reasons that the Secretary of State’s Policy Statement specifically requires the impacts of organisational change on all aspects of safety to be fully assessed and controlled.

### Application

4. This OSA guidance is applicable to all levels of organisational change, from the strategic (Defence organisation) level to the tactical (unit) level. It is recognised and accepted however that the OSA **should** be scaled as required and be proportionate to the proposed change.

5. The management of organisational change naturally focuses on risks that impact the desired outcomes. However, this focus can be blind to unintended consequences such as degradation in the arrangements for managing safety.

---

<sup>3</sup> Safety investigations for example - The Haddon Cave Nimrod Review.2009, which looked into the mid-air fire that led to the total loss of a Nimrod aircraft and the death of 14 service personnel on board, and the investigation into the unassessed changes to the US oil industry regulatory organisation that ultimately contributed to the BP Deepwater Horizon accident which caused the death of 11 workers and had huge environmental impacts.

6. When considering the need to implement organisational change, change owners **must**:
- a. appoint an SRO (at the concept of the change) with the relevant competency and responsibility to undertake an OSA;
  - b. make sure that the SRO undertakes an OSA to assess the impact on the safety risks being managed by an organisation;
  - c. make sure that the SRO undertakes an OSA that is proportionate to the complexity and scale of the proposed change; and
  - d. make sure that the senior leader in a Defence organisation, or delegated individuals, acknowledge any detrimental impact of the change and put in place effective preventative and protective measures to mitigate the risks identified by the OSAs, within their Areas of Responsibility (AoR), to ALARP and tolerable.
7. The SRO is responsible for defining the scope and complexity of the OSA, and how rigorous it needs to be depending on the potential to degrade safety standards, seeking advice from the Safety Centre / CESO or equivalent when required.
8. Where organisational change is initiated that effects another Defence organisation, the wider Defence Operating Model or is pan-Defence in nature, the change owner or SRO of the change **must**:
- a. make sure that the affected Defence organisation's senior leader is informed and the SRO's appointment and OSA responsibilities are agreed and recorded; and
  - b. make sure that the affected Defence organisation's senior leader, or delegated individuals, acknowledge any detrimental impact of the change and put in place effective preventative and protective measures to mitigate the risks identified by the OSAs, within their AoR, to ALARP and tolerable.
9. The SRO **should** consult with the appropriate Safety Centre / CESO or equivalent on the scope and assurance requirements of Defence wide or cross-Defence organisation OSAs. The Safety Centres / CESOs or another department as detailed within the Defence organisation's procedures **should** maintain appropriate records of OSA's for their organisation.
10. The Director General (DG) DSA will provide assurance to the SofS that the safety impact of organisational change within Defence is being appropriately managed through the 3<sup>rd</sup> line of defence (3LOD) assurance process.
11. At the initiation of any change initiative which results in organisational change, the change owner and SRO **should** define how extensive the OSA should be, informed by the potential for the organisational change to impact on safety standards. This is a fundamental and critical decision because it will determine the subsequent nature of the OSA. The change owner **should** be identified in the programme governance arrangements and the SRO **should** be identified as the person responsible for implementing the change programme.

12. The change owner and SRO **should** be able to demonstrate that the OSA is an integral part of any change management programme and:

- a. has been initiated at the concept stage for any proposed change initiative;
- b. is proportionate to the complexity and scale of the change proposal;
- c. remains a live document throughout the change process until it has become business as usual;
- d. has nominated owners and appropriate governance;
- e. is considered as necessary, as part of any wider change programme and its planning process; and
- f. required actions are costed and resourced and are included in the evidence submitted at the programme's approval board as part of the investment approval business case.

13. The SRO **should** formally advise the Safety Centre / CESO or equivalent of the intention to undertake an OSA and **should** be able to demonstrate consultation with the Safety Centre / CESO or equivalent and affected Defence organisations when managing change.

14. The SRO **should** be able to demonstrate that the OSA is comprised of the six phases (see Annex A) that reflect the stages of an organisational change programme and a written record of decisions, assessments and actions at each stage.

15. Typically, the following types of organisational change represent those that have significant potential to impact on the standards of safety:

- a. Changes to Duty Holding arrangements may have a high potential impact on the management of Risk to Life activities. The significance of such changes is such that the relevant Defence Regulator(s) will need to be assured by the OSA that the impacts of any changes are being fully mitigated. It may be that proposed organisational changes to a Duty Holder-facing organisation are also considered by the appropriate Defence Regulator(s);
- b. Major re-organisation of staff or re-alignment of senior management responsibilities. The decision on whether this will influence safety standards will be dependent on the size of the organisation and the levels at which management responsibilities are held. For example, in a strategic headquarters the changes of senior management will have a high potential to impact on safety standards. Within a regional headquarters, the management level of significance could include changes to middle management;
- c. The major re-basing of military equipment capabilities, such as aircraft, military vehicle fleets and maritime assets, may potentially have safety impacts from changes to the routine movement of workforces to significant increases in noise levels;
- d. The transfer of infrastructure and sites from or to another organisation or closure of major Defence sites will result in changes to the management arrangements that may have safety impacts;

- e. Reductions to military and / or civilian staffing levels at a site or across an organisation may impact on the effectiveness of safety management arrangements, which need to be assessed; and
- f. Outsourcing of major areas of Defence enabling or supporting capabilities to industry partners needs to be assessed for any impacts on the management of safety, particularly if there is a proposal to transfer specific responsibilities.

16. Once the change owner or SRO for the proposed change programme has decided that an OSA is required the following six phases of the OSA **should** be followed (summarised in Annex A to this chapter).

### **Phase 1: OSA initiation and declaration**

17. The change owner or SRO for the proposed change programme is to inform the Safety Centre / CESO or equivalent of the decision to undertake an OSA.

This notification is to:

- a. Confirm that the SRO is responsible for conducting the OSA and this is identified in the change programme plan and Terms of Reference (TOR);
- b. Provide the timescale for the proposed change programme including those to achieve Initial Operational Capability (IOC) and Full Operational Capability (FOC);
- c. Describe the governance arrangements for the change programme, such as the stages for approval and by which forum (for example the Investment Approval Board or the Single Service Management Board);
- d. Proposed timescales for the phases of the OSA (for example Phase 2: Baseline or Phase 3: Assessment);
- e. Acknowledge that each phase is to be shared with the Safety Centre / CESO or equivalent with particular note on phases 1, 3, 5 and 6;
- f. Confirmation of the planned date for the OSA to be completed; and
- g. Enclose TOR for the proposed change programme and overarching Level 0 plan.

### **Phase 2: OSA baseline**

18. Where the change owner or SRO has decided that an OSA is necessary it is important that the degree of pre-change safety compliance is established and understood. This will provide the baseline against which the impacts of the proposed changes can be assessed. The baseline can comprise of any relevant information, metrics or data that provides a measure of the effectiveness of the pre-change management arrangements.

19. The mapping procedure **should** be conducted for the understanding of tasks and individuals from both the old to the new organisation, identification of all personnel in the existing and future organisation who will be affected by the change are to be included. This can include core elements of a safety management system (as set out in JSP 815) to assist in identifying potential impacts of change and relevant performance standards and metrics against each element, and any safety maturity assessment, providing that it is evidence-based.

20. Identification of the tasks each person carries out including any tasks secondary to their main duties for example emergency responses, competencies required (any specialist knowledge) or skill that each task or responsibility requires and identify who is accountable and who is responsible for these tasks. It is easy to overlook the loss to the organisation of informal knowledge and processes, personnel often have important knowledge, skills, experience and behaviours (KSEB) and relationships that are not recorded, and which can be lost unless specific effort is made to capture them. A register **should** be maintained of all personnel in the organisation with relevant roles (it **should** also capture contractors).

21. Assess whether the safety arrangements for that organisation including remote (home/hybrid) working are satisfactory and, if not, any shortcomings or lack of resources **should** be identified so that they are not replicated in the new organisation. Staff working excessive hours could be an indicator the current management system is not working effectively. Commanders and managers **should** develop a fallback plan if the changes show signs of increasing safety risks. This may require advising the SRO that certain activities are to cease until control systems are put in place to reduce those risks.

22. The outcome of internal assurance undertaken as part of the first line of defence (1LOD) activity within the last 3 years, trends in lagging safety indicators (number of safety reports, number of injuries, statutory and DSA regulatory enforcement notices) are all suitable sources of information when establishing a baseline.

23. The more comprehensive and detailed the baseline information that is obtained enables a more realistic evaluation of the effects of the change programme on safety. It is easy to focus on the risks to the output of the change programme but the effect on safety is to be fully considered, including second-order effects. Baseline information when collated **should** provide a clear and readily understandable assessment of the existing level of safety compliance.

24. It may not be possible to establish a comprehensive baseline, the setting up of a new organisation / capability is an example where the SRO will need to make a judgement on the best available information. The information to be used might be obtained from how similar organisations work or if several organisations are to be merged into a new Defence organisation using the most relevant data from the current organisations.

25. The change process **should** also be used as an opportunity to examine any stress points in the existing organisation for example records of overtime, workloads, hours of work and individual exemptions from working time regulations, and human factors for example, training (in relation to safety), **should** all be scrutinised.

### Phase 3: OSA assessment

26. Having established an effective baseline, the SRO **should** use the change-sensitive metrics to make an objective assessment of the impact of the proposed organisational change on the pre-change levels of safety. This **should** include the identification of risks and any second-order effects in their own or other Defence organisations. Importantly, this assessment **should** inform the SRO of the choice and costs of mitigations required to address any safety impacts to ensure that they are reduced to ALARP. For example, a significant reduction in the size of the workforce may reduce the management and oversight of safety and this may require mitigation through additional external 3LOD auditing at additional cost.

27. Where mitigations are required to reduce the impact on safety of the change, the SRO **should** make sure that the costs of these mitigations are captured and described fully in the OSA.

28. The OSA baseline and assessment phases can include any reports, data or information collected from various sources, with the information being added directly to the OSA content or copies of the other documentation added as annexes or simply attached as an additional document.

29. Each potential change needs to be considered for its potential impact on the measures captured in the baseline. Where there is no effect from the change, this needs to be documented in the OSA. Equally, where impact is identified the mitigating actions and costs need to be described in the OSA, some examples of this are as follows:

a. **Example 1:** The organisational change may result in the removal of senior posts in the line management chain for the functions that provide advice and 2LOD assurance. Where this results in senior posts assuming more responsibilities, this may reduce the opportunity for advice and audit findings to be brought directly to the attention of the Defence organisation's high level safety committee or management board. The mitigation for this may be to alter reporting lines to ensure safety concerns are raised directly with senior staff. This may not involve any additional costs but would need to be reflected in relevant letters of authorisation and TORs. This finding would need to be detailed in the OSA.

b. **Example 2:** The organisational change may result in the closure of establishments and consolidation of assets, equipment, personnel and activities at larger sites. This may involve short term, large-scale re-basing of assets and construction projects which could cause major disruptions to local communities. In the longer term the transfer of particularly impactful activities, such as fast jet flying, to other geographical locations will have permanent noise impacts on local communities. This may require the investment in local infrastructure and soundproofing of housing, which will require funding. These impacts need to be fully described and costed in the OSA.

c. **Example 3:** The re-organisation of senior management roles removes a senior post which has Duty Holding responsibilities. The baseline organisation and arrangements will need to be revised to ensure the full Duty Holding responsibilities are transferred and held by a suitable and competent senior officer.

30. When the SRO is satisfied the phase 3 assessment is satisfactory the Safety Centre / CESO or equivalent **should** be provided with a copy of the OSA, this is to allow independent overview and feedback to be given, they will advise on the adequacy of the assessment of the impacts on pre-change safety and any proposed mitigations of these impacts before the OSA proceeds to the next phase.

31. The phase 3 OSA **should** be sent to the Safety Centre / CESO or equivalent for review at least one calendar month prior to submission to the change owner (Phase 4), at this point the CESO may consult with the appropriate DSA Regulator for the domain in question. Should further wider regulatory consultation be required, that regulator will take the lead and bring in any additional regulators to obtain input, advice and feedback on the phase 3 review. All feedback **should** be provided to the SRO for consideration and to make any necessary adjustments to the OSA before proceeding.

#### **Phase 4: OSA submission**

32. The SRO **should** include the mitigating actions plan and associated costs described by the OSA in the evidence submitted for the change programme business case for the required funding during the investment appraisal (IA) approval. This will make sure that implications of the proposed change programme on safety and the associated costs of any mitigation are fully considered before approval is given by the change owner for the implementation phase.

33. The OSA **should** also describe the arrangements that the SRO will put in place for assuring that any impacts on the safety baseline are fully mitigated during the implementation of the change programme. When the SRO has submitted the OSA to the change owner for approval the Safety Centre / CESO or equivalent **should** also be provided with a copy of the full OSA. If the change owner is not content that all safety risks have been mitigated so that they are ALARP and tolerable then they will not provide approval for the change to go ahead.

#### **Phase 5: OSA implementation**

34. On approval for the change programme to proceed from the change owner, the SRO **should** provide assurance through audits and monitoring relevant measures of performance and effect that any impacts on the safety baseline are fully mitigated during the implementation phase. Where this assurance reveals new or unforeseen impacts on safety the OSA will need to be reviewed and further mitigations put in place. The change owner is responsible for making sure suitable and sufficient resources are available for the change project to proceed. The SRO assurance activity may be subject to oversight by Safety Centre / CESO or equivalent.

35. The SRO **should** coordinate the effective and frequent cascade of information between all levels of management and personnel during the implementation phase; and make sure the raising of concerns from all levels is supported and encouraged, personnel **should** be provided with feedback following the submission of their concern.

### **Phase 6: OSA review**

36. The OSA **should** be subject to continual review from programme initiation through to FOC, this is to make sure new or emerging risks are captured and assessed, and existing identified risks are all effectively managed and performance measured against the baseline.

37. If conducted correctly, and as an integral part of the change process, the OSA will add value by making sure that the full costs of change are captured and the pre-change safety baseline is not degraded and there are no reputational or operational consequences. Importantly, the assessment of the impacts of the proposed changes **should** also consider impacts on both the organisation's own standards of safety but also those of other organisations that might be affected by the proposed change programme.

38. Once FOC has been achieved and the change programme becomes business as usual a final assessment of the change **should** be carried out, and any additional risk mitigations put in place. Following this final review any further assurance activity will be part of the Defence organisation's routine assurance regime.

### **OSA format**

39. The format of the OSA can vary depending on the complexity of the change programme, as long as the six phases can be identified and recorded for assurance purposes. A narrative text only document can be used, the inclusion of tables and graphs is often helpful to aid understanding, a risk assessment, or a spreadsheet showing the current baseline, the proposed changes, what mitigations are required and then an assessment of any shortfall can be used.

40. Completion of a risk assessment allows the SRO to assess fully the potential impact of an organisational change on existing standards of safety, within both the organisation and on other affected organisations, and any costs that might arise, to provide mitigation where these standards might be degraded. As with all risk assessments, the OSA **should** be undertaken before the organisational change is implemented. In common with all risk assessments (JSP 375 Volume 1 Chapter 8), the OSA **should** be proportional to the potential impact of the proposed organisational change.

41. A template is not provided due to the variation of change programmes that exist; it would not aid the change programme management if the OSA process was an additional bureaucratic burden rather than an integral part of change management.

## Training

42. To help with understanding the general principles of change management in Defence please use the Change Management Training Course that is available to Defence personnel via Defnet.

## Retention of records

43. The OSA and associated documentation are to be retained for a minimum period of 15 years<sup>4</sup> after the change programme has migrated to business as usual. Records **should** be kept in accordance with JSP 375, Volume 1, Chapter 39 (Retention of Records).

## Related documents

44. The following documents **should** be consulted in conjunction with this chapter.

a. JSP 375 Volume1;

- (1) Chapter 2 - Military and Civilian Workplace Safety;
- (2) Chapter 7 - Site Transfer or Closure Procedures;
- (3) Chapter 8 - Safety Risk Assessment and Safe Systems of Work;
- (4) Chapter 17 - Stress in the Workplace; and
- (5) Chapter 39 - Retention of Records.

b. Other MOD Publications;

- (1) JSP 376 – Defence Acquisition Safety Policy
- (2) JSP 815 - Volume 1 and 2.
- (3) JSP 816 – Element 2
- (4) JSP 850 - Infrastructure and Estate Policy
- (5) Infrastructure Operating Model (IOM)
- (6) JSP 418 - Management of Environmental Protection in Defence

c. Legislation and Guidance;

- (1) [Health and Safety at Work, etc Act](#);
- (2) [Management of Health and Safety at Work Regulations](#); and
- (3) [HSE guidance on Human Factors: Organisational Change](#).

---

<sup>4</sup> Retention Schedules - JSP 441 - Information, Knowledge, Digital and Data in Defence (mil.uk)

## Annex A - Six phases of the OSA flow chart

Once the change owner or SRO for the proposed change programme has decided that an OSA is required then they **should** follow the six phases of the OSA, which are:

