Ministry of Defence

JSP 376
Defence Acquisition Safety Policy

Directive & Guidance

Version 1.1
April 2024

Foreword

The Defence Acquisition Safety Policy (JSP 376) has been developed to further Defence's vision for embedding safety within Defence capability. JSP 376 provides Senior Responsible Owners (SROs) and Users clear direction and guidance to support the injection of safety as an enabler from the very onset of programmes, ensuring the progressive management of safety throughout the life of a capability across all Defence Lines of Development (DLOD) through to and including disposal.

JSP 376 builds upon the Defence Safety Management System (JSP 815), codifying acquisition safety requirements and detailing clear safety artefact expectations, while embedding our approach to assessing safety as part of the Defence Investment Approvals process (JSP 655).

The introduction into service of a new capability, or a new solution to deliver an existing capability, is an inherently complex change programme. JSP 376 **simplifies** and **standardises** acquisition safety process where possible. It is vital that safety is not considered as a separate programme element, but as an essential part embedded in all the elements/DLODs to deliver a capability that is 'safe to operate' and can be 'operated safely.'

Similarly, the in-service management will consist of several separate but linked activities that are all required to work together to maintain the capability, while the safe disposal of a capability at the end of its life will involve many activities and stakeholders. JSP 376 therefore seeks to unlock improvements in both military capability and operational readiness through actively eliminating or reducing safety risk early in the development of a capability.

Finally, the successful delivery of safe capability can only be achieved by collaboration between organisations which have a strong safety culture and a psychologically safe environment where staff feel that they can raise safety issues without fear of negative repercussions. Those appointed to be SROs and Users have a personal responsibility to set their programmes up for success by creating these conditions through strong and considerate leadership.

Emma Austen
Director of Defence Safety and Safety Functional Leader

Preface

How to use this JSP

1. JSP 376 provides the MOD organisation and arrangements for the management of acquisition safety in Defence. It is structured in a single part combining the Directive, which provides the direction that must be followed in accordance with statute or policy mandated by Defence or on Defence by Central Government, and Guidance, which provides the guidance and good practice that will assist the user to comply with the Directive.

Terminology

2. **Must, must make sure and should**. Where this policy says **must**, this means that the action is a compulsory requirement to be completed by the actioner. Where the term '**must make sure**' is used, the action may be delivered by an assigned individual, but the actioner remains accountable for these actions being conducted. Where this policy says should, this means that the action is not a compulsory requirement but is considered recommended good practice.

Coherence with other Functional Leadership Policy and Guidance

3. Where this document contains references to policies, publications and other JSPs which are published by other Functions, these Functions have been consulted in the formulation of the policy and guidance detailed in this publication.

Related JSP	Title
375	Management of Health and Safety in Defence
440	The Defence Manual of Security
441	Managing Information in Defence
507	Investment Appraisal and Evaluation
655	Defence Investment Approvals
815	Defence Safety Management System
892	Risk Management
906	Defence Principles for Coherent Capability and Integration
912	Human Factors Integration for Defence Systems
935	Software Acquisition Management for Defence Equipment
936	Dependable Artificial Intelligence in Defence
940	MOD Policy for Quality

Training

4. A review of applicable capability acquisition and acquisition safety training courses has been undertaken by the DDS, with relevant courses documented within the supporting Frequently Asked Questions document. This list of relevant courses is non-exhaustive. For further information and guidance, please contact COO-DDS-ASC-GroupMailbox@mod.gov.uk.

Further Advice and Feedback – Contacts

5. This JSP will be reviewed at least annually. The owner of this JSP is Director of Defence Safety (Dir DS). For further information or advice on any aspect of this publication

or to provide feedback on the content, contact: COO-DDS-ASC-GroupMailbox@mod.gov.uk.

Amendment Record

6. Amendments will be staffed by the DDS together with lead areas, relevant subject matter experts and key stakeholders.

7. Comments or proposed amendments to this JSP are to be made by e-mail to COO-DDS-ASC-GroupMailbox@mod.gov.uk using the following format:

a. subject: JSP 376 proposed amendment;

b. sender's reference;

c. date;

d. chapter, page and paragraph being addressed; and

e. comment.

Version No	Date	Comment	Authority
1.0	Jul 23	Initial release	Dir DS
1.1	Apr 24	Minor updates	Dir DS

Disclaimer

8. Nothing contained within this JSP removes the requirement on anyone to comply with applicable Statutory legislation, the Secretary of State for Defence Policy Statement on Health, Safety & Environmental Protection or Defence safety regulations.

Equality Analysis Impact Statement

The policy in this JSP has been equality impact-assessed in accordance with Departmental policy.

Contents

Annexes:

1 Introduction

Purpose

1. The purpose of JSP 376 is to **standardise** and **simplify** Defence's approach to acquisition safety, setting the SRO/User up for success throughout the acquisition lifecycle to deliver capabilities that are 'safe to operate' and, beyond the introduction of a military capability into service, make sure capabilities are 'operated safely'. It does this by providing:

- a standardised approach to acquisition safety across Defence, making sure that safety is actively considered from the outset at programme-level.
- clarity to safety accountabilities and responsibilities, amplifying the acquisition safety requirements set out within the Defence Safety Management System (JSP 815).
- direction and guidance for how safety is to be treated as an enabler for military capability alongside other performance criteria.
- clear safety expectations and evidence requirements consistent with Defence Investment Approvals (JSP 655) and the broader approvals decision support and assurance obligations.

2. JSP 376 frames acquisition safety around six key concepts (Chapter 2):

- Safety Management.
- Safety Requirements.
- Test & Evaluation (including Certification).
- Safety Case.
- Supervision and Control Activities.
- Acquisition Safety Assurance and Approvals Decision Support.

and then explains how they are to be applied across the acquisition lifecycle (Chapter 3).

3. Proportionality is a fundamental attribute of effective risk management. Where possible, JSP 376 seeks to avoid prescribing approaches or requirements as these may not be proportionate. Rather, JSP 376 sets goals and provides guidance on what good would look like. This enables Defence organisations, SROs and Users to tailor how they meet the policy requirements based on the size, complexity and safety risk of the programmes.

Scope

4. The direction and guidance contained in JSP 376 applies to all acquisition programmes delivered in all Defence organisations.

Terms and Definitions

5. The following paragraphs provide an overview of the key terms and definitions used within this policy. General safety terms and definitions are provided in the Master Terms and Definitions Glossary which can be accessed via the gov.uk webpage.

6. **Acquisition Safety**. Acquisition safety is a term used within the MOD to describe the application of management principles and techniques to deliver a capability that is 'safe to operate' and can be 'operated safely' throughout the acquisition lifecycle (procurement, operation and disposal).

7. **Senior Responsible Owner (SRO)**. As per JSP 655, where JSP 376 uses the term SRO, it refers to the individual who is accountable for delivery of the programme[1]. In the early stages of a programme, this role could be filled by individuals in different job roles such as a Capability Sponsor or Transformation Manager where an SRO has not, or has not yet, been formally appointed.

8. **SRO/User**. Where this policy uses the term 'SRO/User', this means that the action is applicable to either the SRO or User. It is recognised that the individual who is accountable is often dependent on the stage of the acquisition lifecycle (e.g. generally, an SRO will be accountable up to the point that the capability enters service, with the User accountable for actions thereafter). Where accountability is unclear in the first instance, the SRO and the User are required to consult with one another to make sure that they agree who is accountable for the action. For any further clarification, please engage with Directorate of Defence Safety (DDS) Acquisition Safety Cell (ASC).

9. **Programme.** JSP 376 also uses the term programme to describe the management construct within which the required change outcome is delivered. In this respect, the term programme refers to the pan-DLOD[2] aspects for which an SRO is accountable. The terms project or element refer to specific aspects of a programme which an SRO may choose to assign to another organisation or individual but remains accountable for.

10. **Head Office Approvals**. JSP 376 sets out how Approving Authorities (AA) are supported in their decision making at the key decision points by the provision of independent safety advice. Dir DS has been appointed as the safety advisor to the Head Office Investment Approvals Committee (IAC)[3] and is supported in this role by the Acquisition Safety Cell (ASC)[4]. For simplicity, JSP 376 is written to primarily focus on the safety approvals decision support that the Head Office IAC is provided by Dir DS and the ASC.

11. **Delegated Approvals**. While JSP 376 is written to primarily focus on programmes that require investment approval by the Head Office IAC, JSP 376 also requires equivalent measures to be put in place by Defence organisations for any delegated AA[5]. Therefore, where JSP 376 uses the terms AA and ASC, it refers to both submissions to the IAC and any delegated AA, and the safety approvals decision support capacities put in place by Defence organisations.

Safety Legislative Requirements

12. Health and safety legislation requires that safety risks be assessed and reduced to an As Low As Reasonably Practicable (ALARP)[6] level, with secondary legislation setting prescribed limits for managing some hazards.

---

[1] JSP 655, Part 1, Paragraph 12.
[2] The Defence Lines of Development are Training, Equipment, Personnel, Information, Concepts & Doctrine, Organisation, Infrastructure, and Logistics (TEPIDOIL), with Interoperability as an overarching theme.
[3] Throughout this policy, reference to the IAC also applies to the IAC(Nuclear).
[4] The Acquisition Safety Cell is part of the Directorate of Defence Safety in Head Office.
[5] See Chapter 2, Acquisition Safety Assurance and Approvals Decision Support, for further information.
[6] Health and Safety at Work etc Act 1974.

13. **Recognised Good Practice**. The starting point for demonstrating that risks are ALARP will normally be to implement risk controls that are recognised as good practice. The Health and Safety Executive (HSE) defines good practice as the 'measures we would normally expect to see in such circumstances', i.e. for a similar capability in a similar context.

14. **Cost Benefit Analysis**. In some cases, where the benefits do not clearly outweigh the costs or it is not clear which option is most effective, it will be necessary to make an assessment of the amount by which the safety risk will be reduced and the effort or sacrifice to do so. This sacrifice can take into account the time necessary to implement a control measure, or its operational implications, as well as purely financial costs. The comparison must be in favour of safety, so that risk control measures are implemented unless they are grossly disproportionate. The Defence Investment Appraisal and Evaluation Policy (JSP 507) provides direction and guidance on the use of cost benefit analysis in support of ALARP decisions. Given some of the complexities associated with ALARP considerations, Defence Economics should always be contacted prior to any ALARP cost benefit analysis being conducted.

15. **Statutory Requirements/Standards**. The SRO is required to make sure that the appropriate statutory requirements and standards are identified and met, including the requirement to demonstrate that the safety risks are ALARP. In certain circumstances, Defence may rely on an exemption where it is not possible to meet the statutory standards and still deliver the required military capability. In such circumstances, which should only be used when all other courses of action have been considered and discounted, the SRO is responsible for consulting with the User, justifying the case and sponsoring such an exemption in accordance with JSP 815, Volume 2, Annex B (Exemption Certificate Process). Where a need for an exemption is identified after the capability has entered service, for example due to a change in the capability or legislation, the User is responsible for sponsoring an application for such an exemption.

16. **Risk Tolerability**. In addition to the legal requirement to reduce safety risk to an ALARP level, there is also a need to consider whether the residual safety risk is Tolerable. Tolerability of risk is a wider consideration than just whether the risk is acceptable by those directly affected and takes into account whether the risk would be considered acceptable to wider society. It may therefore be possible that a safety risk has been reduced to ALARP as there are no further practicable risk reduction measures available, but the risk may not be Tolerable as it would not be seen as acceptable by wider society. Therefore, the SRO/User is required to consider whether a residual safety risk is both ALARP and Tolerable.

17. **Hierarchy of Controls**. Another core component to demonstrating that residual safety risks are both ALARP and Tolerable is the use of the hierarchy of controls[7]. As a method of determining which measures will best protect personnel from hazards, the hierarchy is arranged from the most to least effective. During the initial phases of the acquisition lifecycle, there is the greatest opportunity to identify and embed control measures, with risk reduction strategies often including new safety requirements (e.g. the incorporation of protective functions).

[7] JSP 375, Volume 1, Chapter 8 (Safety risk assessment and safe systems of work)
Elimination – physically remove the hazard
Substitution – replace the hazard
Engineering controls – isolate people from the hazard
Administrative controls – change the way people work
Personal Protective Equipment – protect the worker with equipment.

Defence Acquisition Safety Policy Framework

18. The Defence Acquisition Safety Policy Framework is shown in Figure 1. JSP 376 provides Defence-level, pan-domain policy on how acquisition safety is to be implemented, drawing together the requirements of the wider Defence safety policy contained in JSP 815 and Defence acquisition policy, in particular JSP 655.

Figure 1 - Defence Acquisition Safety Policy Framework

19. The DDS owns Defence Safety Policy, including the overarching Defence Safety Management System (JSP 815). Defence safety regulations[8] are developed and managed by the Defence Safety Authority (DSA), as an independent Enabling Organisation, within a safety management system owned by DDS on behalf of SofS. The DSA, through their regulations, are responsible for providing direction and guidance on the implementation of JSP 376 at domain-level. Thereafter, Heads of Defence organisations are responsible for providing direction on the implementation of these policies within their organisations. Standards such as Defence Standard 00-056 set out requirements and guidance for the achievement, assurance and management of safety for use by Defence organisations when contracting for services with industry.

Safety within Capability Management

20. The through-life management of capability is dependent on the capability being planned, delivered and maintained in a state that is both 'safe to operate' and 'operated safely'[9]. Heads of Defence organisations[10] are required to make sure that safety is explicitly considered as part of the 'Develop' function by the Capability Sponsors alongside other key factors when developing their Capability Management Strategies and subordinate Capability Management Plans, and within associated capability governance structures[11].

Safety within Acquisition Programmes

21. Figure 2 illustrates the Programme Delivery 'Iron Triangle', where the programme delivery envelope across all DLODs is defined in terms of Performance (sometimes also referred to as Quality), Cost and Time (PCT) parameters. Changes in one parameter can

[8] Defence safety regulations are a specialist form of Defence policy where the MOD has Disapplications, Exemptions, and Derogations (DEDs) as set out in relevant legislation or other circumstances indicate the need for Defence regulation of activities.
[9] Throughout this policy, the terms 'operate' and 'operated' refer to, but are not limited to, use, maintenance, repair, storage, transportation and disposal of a capability.
[10] Including Defence Nuclear Organisation (DNO) and Strategic Programmes.
[11] For example, Capability Management Groups.

result in the need to change others to allow the programme to continue to deliver the required capability.

22. Safety is a key element of the Performance parameter and is required to be considered alongside other performance requirements. Changes to the Cost and Time parameters, or changes to other Performance parameters, of any element of a programme can have an impact on safety.

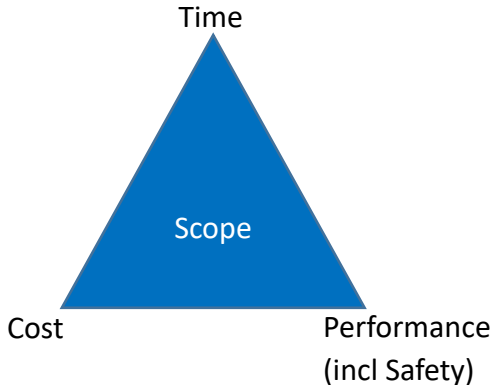


Figure 2 - Safety in the Programme Delivery 'Iron Triangle'

23. The SRO is required to make sure that safety implications across all DLODs are considered from the outset of programmes, enabling safety issues to be eliminated or mitigated through early design choices. By injecting a safety perspective and culture into acquisition programmes from the outset, Defence can unlock improvements in both military capability and operational readiness and reduce the risk of safety issues materialising later in the acquisition lifecycle.

24. **Internal Interfaces**. While the SRO/User is accountable for safety across the whole programme, they will appoint suitably qualified, experienced and empowered individuals to deliver elements/projects within the overall programme, including responsibility for safety within that element/project. In addition to providing oversight of element/project-level safety, the SRO/User should pay special attention to safety at the interfaces between elements/projects to make sure that safety is delivered/maintained in a coherent manner at programme-level.

25. **External Interfaces**. Beyond the programme for which they are accountable for, the SRO/User should also account for safety at interfaces between programmes. This includes interfaces with new programmes, on-going programmes, and existing programmes where a capability may be in-service. Tight control of dynamic interfaces is essential to achieving the delivery of a capability that is both 'safe to operate' and 'operated safely'.

26. **Personnel Competence, Resources and Training**. It is important that an individual's safety competence is matched to their role and accountability throughout an acquisition lifecycle. Many policies, regulations and standards require use of a 'competent person', 'Suitably Qualified and Experience Personnel (SQEP)' or personnel with 'the relevant safety skills, knowledge, experience and behaviours (SKEB) and expertise requirements' to carry out a specific task or hold a specific safety authority. Whilst SROs and Users are personally accountable for their responsibilities, it is it vital that they are supported by competent and authorised individuals. JSP 815, Volume 2, Element 6 provides Defence organisations with direction and guidance relating to personnel competence, resources and training.

27. **Safety Leadership**. The role SRO/User for a major capability programme in MOD is challenging. Successful capability acquisition (including successful procurement,

operation and disposal) hinges on the attitudes and behaviours of the leadership and people in the organisation throughout the life of the capability. The SRO/User has a personal responsibility to make sure that safety is considered at all times alongside the other aspects of the programme. To deliver this requirement:

- **Safety Culture**. The SRO/User is required to make sure that a strong Safety Culture[12] exists throughout the acquisition programme, encouraging safety through the values, attitudes and behaviours shared throughout an organisation.
- **Collaboration**. While this policy places primary responsibility on the SRO/User, safe capability acquisition relies on a close working relationship between all stakeholders, including the capability sponsor, delivery agent(s), operators, industry, any safety regulatory organisations and Approving Authorities. The SRO/User is therefore required to establish and maintain a positive and collaborative environment within which the capability can be safely delivered.
- **Psychological Safety**. The highest performing teams operate in a psychologically safe environment. Research shows that the behaviour of leaders is essential for enabling these conditions[13]. The SRO/User is required to create an environment across the whole programme where all staff can raise safety concerns without fear of negative repercussions.

Acquisition Safety Lifecycle

28. MOD uses as acquisition lifecycle based on the six phase CADMID/T cycle – Concept, Assessment, Demonstration, Manufacture, In-Service, and Disposal/Termination, with the addition of a Pre-Concept Phase to align with the Treasury Green Book Appraisal and Evaluation policy. Each of the seven acquisition phases involves executing the plan agreed in the previous phase, reviewing the outcome, and planning for the remaining phases. The end of the first three phases is marked by a formal decision by an Approval Authority to move forward to the next phase based on the evidence submitted in a Business Case (BC)[14], with supporting evidence as required.

29. Safety activities are undertaken throughout the life of a capability, but it is essential that the right ones are done at the right time to make sure that a 'safe to operate' capability is delivered into service and that it is 'operated safely'. This policy outlines the high-level safety requirements during each phase in the acquisition lifecycle.

30. There is greatest opportunity to influence and embed safety into the capability acquisition process during the initial stages. Effort is well spent in the identification of relevant requirements and standards, potential safety risks and the planning of mitigation measures through concept development and solution design. Leaving this to the later stages where the mitigation options available are more limited and could have greater impact on programme performance, cost and time.

[12] See JSP 815, Volume 2, Element 1 (Leadership, Governance and Culture).
[13] Psychological Safety in MOD Major Programmes Report dated July 2022.
[14] Strategic Outline Case (SOC) at end of Pre-Concept Phase; Outline Business Case (OBC) at end of Concept Phase; Full Business Case (FBC) at end of Assessment Phase.

31. This phased development of safety through the acquisition lifecycle is presented in Annex B, along with a graphical depiction of Safety Case (SC) and Safety Management System ownership, which is discussed in the following sections.

32. The SRO/User will apply the standard acquisition lifecycle in a flexible and agile way to deliver and maintain the required capability. Similarly, the SRO/User will need to apply the requirements of this policy in line with their application of the overall acquisition lifecycle, including demonstrating so as part of the BC approval process. The SRO/User should pay particular attention to the running of acquisition phases in parallel, recognising that concurrent phases may add complexity, technical risk and safety risk into the programme.

Safety within Acquisition Reform

33. JSP 376 is coherent with the wider Acquisition Reform Programme and supplements the range of work being undertaken across Defence to address acquisition challenges. The Acquisition Reform Programmes comprises of five themes designed to drive pace in delivery to the front-line. JSP 376 supports these themes as follows:

- **Cost estimating and cost control.** JSP 376 will make sure that costs associated with acquisition safety activities are estimated, accounted for, and controlled by programmes from early in the programme and through-life.
- **Relationships with industry.** JSP 376 reinforces the importance Defence places on acquisition safety, driving greater oversight and transparency on safety risks throughout the acquisition lifecycle. This will enable clear engagement with industry to deliver and support safe capability.
- **Linking requirements to strategic intent.** JSP 376 codifies the approach to acquisition safety management, making sure that safety is actively considered alongside other strategic factors from the outset of programmes.
- **Empowering and enabling programme leadership.** JSP 376 provides the SRO and their programme teams with a clear understanding of the safety requirements and expectations across the acquisition lifecycle. Including safety within the performance parameters of the programme allows it to be appropriately prioritised and managed by the SRO/User.
- **Systems, accountabilities and processes.** JSP 376 makes sure that safety accountabilities and responsibilities are clearly understood across the programme, including where elements/projects are assigned to Delivery Agents or contracted to industry.

Non-standard Acquisition and Innovative Technologies

34. With capability acquisition continually evolving across Defence, the following paragraphs provide direction and guidance on the use of non-standard acquisition methodologies and innovative technologies embedded within solution procurement and design. Further details of the application of safety policy requirements on the use of non-standard acquisition methodologies will be developed for later versions of this JSP.

35. **Agile and Adaptive Acquisition**. The acquisition safety responsibilities of the SRO remain unchanged within adaptative acquisition approaches. The SRO is required to make sure that all programme delivery, including that delivered by adaptive acquisition approaches, is compliant with acquisition safety policy requirements. The SRO is required to make sure that all outputs delivered for use, be they interim or final standard

deliverables, comply in full with all appropriate safety requirements, supported by evidence in the form of a SC and associated safety documentation. Where this is not possible due, for example, to the early development of the solution, the SRO is required to engage early with the appropriate statutory and Defence authorities to make sure that the required exemptions, waivers or concessions are put in place before the capability is brought into use.

36. **Innovation and Experimentation (I&E)**. I&E are an important part of the capability acquisition process, be they conducted prior to a formal programme being commissioned or as part of such a programme. In many cases, early solution prototypes will be operated in novel ways to expedite the development, experimentation and trial of new concepts. In planning for I&E activity, safety accountabilities and responsibilities should be agreed and documented. Those accountable for I&E activity are required to make sure that a suitable and sufficient risk assessment is conducted before any activity takes place. Furthermore, they are also required to make sure that one of the outputs of the I&E activity is the identification of and assessment of how the capability will be able to meet the safety requirements as the programme moves through the acquisition process. Particular attention should be paid to future certification requirements.

37. **Programmable Elements/Software**. The safety of the programmable elements within solutions can cause significant problems, often because software, firmware and data are not visible to the operator and the faults which they can cause appear unfamiliar and unpredictable. Faults within programmable elements can lie dormant, waiting for a 'revealing mechanism' such as an unexpected input or a change in operating conditions, before enacting hazardous consequences or informing operators to make unsafe decisions. The SRO/User is required to follow the Software Acquisition Management for Defence Equipment policy (JSP 935) in acquisition of software, and make sure that the techniques that aid the development of safe software and data are properly implemented. Defence Standard 00-055[15] focuses on providing the MOD with confidence that the programmable elements used in safety-related applications will behave appropriately.

38. **Cyber Security.** A system cannot be trusted to be safe if it is not secure. Although safety and security objectives do not always align, the increased use of software and network-enabled capability means that security, and in particular cyber security, is becoming ever more important to ensuring safety. The SRO/User is required to make sure that there is dialogue throughout the programme lifecycle between those managing safety and those managing the security aspects of the capability, taking a 'Secure by Design' approach to capability acquisition. The Defence Manual of Security (JSP 440) provides direction and guidance on cyber security.

39. **Autonomous Systems and Artificial Intelligence**. Autonomous systems and artificial intelligence have the potential to revolutionise capabilities, not least with the removal of humans from dangerous situations or places. However, with systems being able to make decisions independently of human control, there are many uncertainties and risks that need to be carefully managed. The SRO/User is required to make sure that the safety assurance of autonomous systems is actively considered, making sure that appropriate models are used to provide justified confidence or certainty in a systems capability. For further information on artificial intelligence, please refer to the Dependable Artificial Intelligence in Defence policy (JSP 936).

[15] Requirements for Safety of Programmable Elements in Defence Systems.

Key Acquisition Safety Responsibilities

40. **SRO**. The SRO is a programme delivery appointment and will usually sit within one of the Military Commands, Defence Nuclear Organisation (DNO), or Head Office Strategic Programmes. The SRO is the person accountable for programmes meeting their objectives, delivering the proposed outcomes, and realising the required benefits[16]. From a safety perspective, the SRO is accountable for delivering a capability that is 'safe to operate' and that activities undertaken to do so are conducted safely. This includes setting the safety requirements and contracting for safety, assuring that the capability meets the requirements laid down within applicable legislation, regulation and standards. The SRO is accountable for putting in place mitigation measures based on the hierarchy of controls to make sure that residual safety risks can be declared as ALARP and Tolerable and that those residual safety risks are communicated to the User.

41. **User**. The User will usually sit within one of the Military Commands and is the person accountable for the capability being maintained in a 'safe to operate' condition and is 'operated safely'[17]. This includes making sure that activity is supported by a suitable and sufficient safety risk assessment within an appropriate safe system of work, and that the residual safety risks are clearly understood and communicated to the capability operators. The User is accountable for making sure that the capability is operated in accordance with the defined method of use, within the defined operating envelope, in the agreed configuration and maintained in accordance with procedures. This includes the provision of suitable and sufficient information, instruction, training, and supervision is provided, and that safety incidents are reported and investigated, in accordance with the relevant Defence policies.

42. **Test & Evaluation (T&E) User**. The T&E User is the person accountable for the capability being 'operated safely' where T&E activity is controlled by MOD. The T&E User may be the User, from the same Defence organisation as the User, or someone from a different Defence organisation. The T&E User has the same safety accountabilities for the T&E activity as the User has for in-service activity.

43. **Lead User**. Where a capability has more than one User (e.g. where a capability will be used by multiple Military Commands), the Lead User is the person accountable for fulfilling the responsibilities of the User detailed in this JSP in consultation with all User Defence organisations. Where the term User is used in this policy, this therefore also refers to a Lead User (where appointed).

44. **Approving Authority.** The Approving Authority is the person or committee who has the authority to give approval for an investment decision. For further information on Approving Authorities, please refer to JSP 655.

45. **Requirements Oversight Committees (ROC)**. There are various ROC throughout Defence, including a Joint ROC (JROC) and Defence organisation specific ROCs. ROCs confirm that the requirement, or programme scope, is sufficiently understood, valid, aligned with other capabilities within the Defence portfolio, and deliverable across all DLODs. From a safety perspective, the relevant ROC can help shape High-Level Characteristics (HLC) and Key User Requirements (KUR) to make sure that the safe intent is captured. For further information on the ROCs, refer to JSP 655.

---

[16] https://www.gov.uk/government/publications/the-role-of-the-senior-responsible-owner/the-role-of-the-senior-responsible-owner.

[17] Where enhanced safety management arrangements are required, the User may also be a Duty Holder, as described in JSP 815, Volume 2, Element 5 (Supervision, Contracting and Control Activities).

46. **Approvals Decision Support Community**. The Approvals Decision Support Community exists to support the investment decisions that are made by the relevant Approving Authority through expert independent analysis and advice. For further information on the Approvals Decision Support Community, refer to JSP 655.

47. **Delivery Agents**. In most cases, the SRO/User will engage with Delivery Agents for the delivery of elements of their programmes, including the management of contracts with industry to provide the products, services and systems required to meet the SRO/Users' requirements. As such, Delivery Agents are likely to be responsible for delivering much of the necessary safety evidence required by this policy to enable the SRO/User to demonstrate that a capability is 'safe to operate'. Within Defence, four of the Enabling Organisations are set up specifically to conduct the Delivery Agent role[18]. However, the SRO/User may decide to use other Defence organisations, parts of their parent Defence organisation, or conduct the delivery agent role from within their own team. In all cases, the SRO/User is required to make sure that the Delivery Agent's safety responsibilities are articulated in the programme safety management plan and any supporting responsibility assignment documentation (e.g. Command Acquisition Support Plans (CASPs)).

48. **Defence Safety Authority**. The DSA is independent from Defence activity, as set out in the DSA Charter. The DSA leads on Defence Health, Safety and Environmental Protection (HS&EP) regulation and provides independent assurance to the Secretary of State through the Permanent Secretary. With respect to acquisition safety, the DSA provide domain specific regulatory requirements which Defence programmes are required to follow and against which DSA will conduct assurance.

49. **Director of Defence Safety**. Dir DS has responsibility for Safety Functional Leadership across Defence on behalf of the Chief Operating Officer (COO). Dir DS owns the overarching Safety Management System (JSP 815) and is responsible for the corporate governance of Defence Safety on behalf of the Permanent Secretary. Specific to acquisition safety, Dir DS has been appointed as the IAC, JROC and Defence Major Projects Portfolio (DMPP) Sponsor Group's permanent safety advisor and is supported in this role by the ASC.

50. **Acquisition Safety Cell (ASC)**. The ASC forms part of the DDS and provides an approvals decision support role for acquisition safety. Primarily focused on high risk and complex programmes, the ASC is a functional member of the Head Office Approvals Decision Support Community. The ASC supports investment approvals through the provision of independent analysis and advice on whether a programme is being managed in accordance with JSP 376. The advice provided draws upon existing safety-related programme artefacts and does not express an opinion on the safety of the programme's outputs or outcomes.

[18] Defence Equipment and Support (DE&S), the Submarine Delivery Agency (SDA), Defence Digital and the Defence Infrastructure Organisation (DIO).

2 Key Concepts

Safety Management

Key Policy Statement – Safety Management

The SRO/User must make sure that a Safety Management Plan (SMP) is put in place to describe how they intend a capability to be safely delivered, operated, and disposed of, in accordance with the parent organisations Safety Management System (SMS).

1. Safety management is a critical element of programme management. The application of a structured safety management process will help make sure that a comprehensive safety approach is planned and implemented.

2. The HSE[19] and JSP 815 recommends the adoption of the Plan-Do-Check-Act cycle as the structure for an SMS. This structure is as applicable to safety management in change programmes, including capability acquisition, as it is for routine business.

Plan

3. Safety management is one aspect of the overall programme management. The SRO **must make sure** that safety is included in the overall Programme Management Plan, and key safety tasks are included in the Programme Integrated Master Schedule.

4. The SRO/User **must make sure** that a SMP is established and maintained for each programme. The SMP should sit within the context and safety management arrangements detailed in the parent organisation's SMS[20] and detail the way in which safety will be managed across all programme elements/DLODs in support of the delivery and use of the required capability[21]. The SMP should be proportionate to the size, complexity and safety risk of the programme. The SMP should typically include, but is not limited to:

- a brief description of the capability that the programme will deliver;
- key programme safety requirements;
- safety deliverables and milestones, such as the Safety Case Report (SCR) and the provision of suitable and sufficient safety evidence, including Certification where required;
- safety structures, roles and responsibilities, including safety competence requirements. The assignment of safety responsibilities may need to be supported by formal letters of appointment/delegation and terms of reference (or equivalent);
- an overview of the programme's safety governance arrangements, including the way in which safety is accounted for within the management of change;
- the safety risk management process, including safety risk escalation;

[19] Managing for health and safety (HSG65).
[20] E.g. ACSO 1200, ACSO 1201, BRd 10, AP8000.
[21] Note that the programme SMP is different from the Delivery Agent Delivery Team SMP, which may be focussed on the project-level delivery of specific DLOD elements of the programme (e.g. equipment). Other DLODs may also have their own SMPs for the project delivery of their elements of the programme.

- the safety assurance process, including the use and monitoring of safety performance indicators.

Do

5. The SRO/User **must** implement the SMP if the programme is to deliver and maintain a safe capability. Key to implementation is:

- Safety risk management, which focuses the programme on identifying and addressing the key safety risks within the context of overall programme delivery. In addition to being held in a specific safety risk register, key safety risks are required to be included in the programme Risk Register and given suitable and sufficient weighting alongside other programme risks.

- Strong safety governance, which holds to account those with safety accountabilities for the delivery of the relevant safety outputs.

Check

6. The SRO/User **must** constantly monitor the development and maintenance of the safety elements of the programme as an integral part of the programme governance. Further details can be found under the Acquisition Safety Assurance and Approvals Decision Support Key Concept.

7. When accidents, incidents or near misses occur, the SRO/User **must make sure** they are thoroughly investigated to make sure that the applicable lessons are identified[22]. This includes the investigation of incidents during test and evaluation activity, which will have a significant impact on safety further down the programme and into the In-Service Phase.

Act

8. The SRO/User **must make sure** that actions resulting from monitoring performance, recommendations made from assurance activity (including actions based on regulatory enforcement) and lessons identified from investigations are properly implemented to make sure that a safe capability is delivered and, once delivered, the ALARP and Tolerable status is maintained.

Organisational Safety Assessment

9. Supporting the requirement that organisational changes are evaluated, risk assessed, approved and documented[23], JSP 375, Volume 1, Chapter 35 (Safety and the management of change) provides direction and guidance to Defence organisations on the production of an Organisational Safety Assessment (OSA). An OSA identifies the potential safety risks of a proposed change and the required control measures to manage those risks to make sure that there is no adverse impact to the health and safety of personnel or the safe conduct of Defence activities[24]. Organisational change is wider than just changes to organisational structures and encompasses pan-DLOD changes affecting the structure or range of duties currently conducted by personnel within that organisation.

10. The introduction of a significant new capability solution is likely to fall within the scope of such organisational changes. The production of the SC for the new capability will be an

[22] JSP 375, Volume 1, Chapter 16 (Accident/Incident Reporting and Investigation).
[23] JSP 815, Volume 1, Element 2, Expectation 2.7.
[24] JSP 815, Volume 2, Element 2, Paragraphs 16-20.

important part of the OSA process, providing evidence that the safety risks of the new capability solution are ALARP and Tolerable. The SRO **must** formally consider the need for an OSA during the procurement phases of the programme and be able to justify the decision if they consider that an OSA is not required. Similarly, the User **must** formally consider the need for an OSA when there are in-service changes to the capability, including changes to how the capability is used as well as changes to the capability itself. Where an OSA is undertaken the SRO/User should include a clear declaration that there is no reasonably foreseeable detriment to safety as a result of the proposed change.

Safety Responsibilities

11. For safety to be successfully managed on a through-life basis, the SRO and User **must** closely engage with one another as early as possible, and throughout, the acquisition process. The SRO **must** seek, and the User **must** provide, input to the programme from an in-service perspective, noting that the User will be accountable for safely delivering the programme benefits and integrating the programme outcomes with other military capabilities.

12. For some programmes, especially those for new capabilities, the User may not have been formally appointed or exist early in the acquisition cycle. In such cases, the SRO **must make sure** that arrangements are made for in-service input to be provided, even though the provider of that input may not become the actual User in due course.

13. The SRO/User **must make sure** that safety authorities, accountabilities and responsibilities are documented within the SMP, appropriate letters of appointment/delegation and terms of reference (or equivalent), and that staff are competent for those roles. The SRO/User **must make sure** that safety responsibilities assigned to industry providers are included in contractual arrangements. This documentation starts from the SRO's Appointment Letter down and, for key responsibilities, should be acknowledged and accepted in writing.

14. **Lead User**. Where a capability is to be used by more than one User, Heads of Defence organisations **must make sure** that a Lead User is agreed and appointed who has responsibility for consultation with and representing the views of the other User Defence organisations throughout the acquisition lifecycle.

Digital Engineering

15. The adoption of digital technologies has the potential to improve programme performance, including the acquisition process (for example by using digital twins/mathematical models to reduce the amount of live testing and to support certification), enhancing operational availability (for example by using live data feeds into a digital twin to improve platform status understanding) and the improve supporting business processes (for example by producing digital SCs to improve data sharing). The SRO/User should actively consider using such Digital Engineering tools, engaging with the relevant authorities (e.g. Certification Bodies, etc.) early to agree the use of such tools, always noting the need to manage the programme safely and provide an evidence-based argument that the capability is 'safe to operate' and can be 'operated safely'.

Quality Assurance

16. There is an intrinsic link between quality and safety, with safety often considered to be one of the multiple domains of quality. In accordance with the MOD Policy for Quality (JSP 940), proportionate, robust and rigorous processes are to be put in place to assure the quality

of products, services and systems supplied to the MOD. These processes are required to assist the MOD to get the product, service or system ‘right first time’, as well as provide appropriate feedback to supply chain and suppliers when defects are discovered. Particular attention should be paid where there are products, services and systems that are considered to be ‘safety critical’ within the programme.

Information Management

17. Effective management of safety information is required throughout the life of a capability to sustain a SC and contribute to the delivery of safe operations. Without a systemic approach to the management of safety information, whether using a paper-based system, an electronic system, or a combination of the two, the SC will be undermined. It is important to make sure that the evidence underpinning a SC can be accessed easily when required; and that the information needed to control residual risks is made available to the people who need to know it and kept up to date. The SRO/User **must make sure** that the information used to establish and sustain a SC is defined within the SMP, alongside the way this information is managed in accordance with the policy for Managing Information in Defence (JSP 441), JSP 375 Volume 1, Chapter 39 (Retention of records) and any relevant Defence safety regulations.

Safety Requirements

Key Policy Statement

The SRO must make sure that the User Requirements Document (URD) captures all safety User Requirements (URs) and reflects the need for the capability to be both 'safe to operate' and 'operated safely' for a given application in a given operating environment.

18. All programme requirements, including safety requirements, should stem from a set of capability requirements and be set in the operating context as defined by the Concept of Employment (CONEMP) and thereafter the Concept of Use (CONUSE), which should be developed early in the programme as part of the Concepts and Doctrine DLOD. From these documents, the SRO will develop the programme Single Statement of User Need (SSUN) and capability High-Level Characteristics (HLC).

19. **Key User Requirements (KUR)**. For high risk and complexity programmes, the SRO **must** include a candidate safety KUR. For lower risk and less complex programmes, the SRO **must** formally consider the need for a safety KUR. Where the SRO does not consider the need for a safety KUR, they **must** be able to justify that decision to the appropriate ROC and AA as part of the Strategic Outline Case (SOC) and Outline Business Case (OBC) submissions. The SRO should discuss the need for, and the structure of, safety KURs with the ASC.

20. **User Requirements**. In alignment with the Vision for Safety in Defence, safety is treated as an enabler for military capability and is therefore reflected within the URD under 'Performance' (see Figure 3). Safety URs should be Specific, Measurable, Achievable, Relevant and Timed (SMART), and developed through early, widespread, stakeholder consultation with the User and other interdependent capabilities. Safety URs should be developed with input from Human Factors analysis[25]. The SRO **must make sure** that an audit trail of safety requirements is maintained. The audit trail should document the time, date and status changes of requirements, including rationale for any changes made.

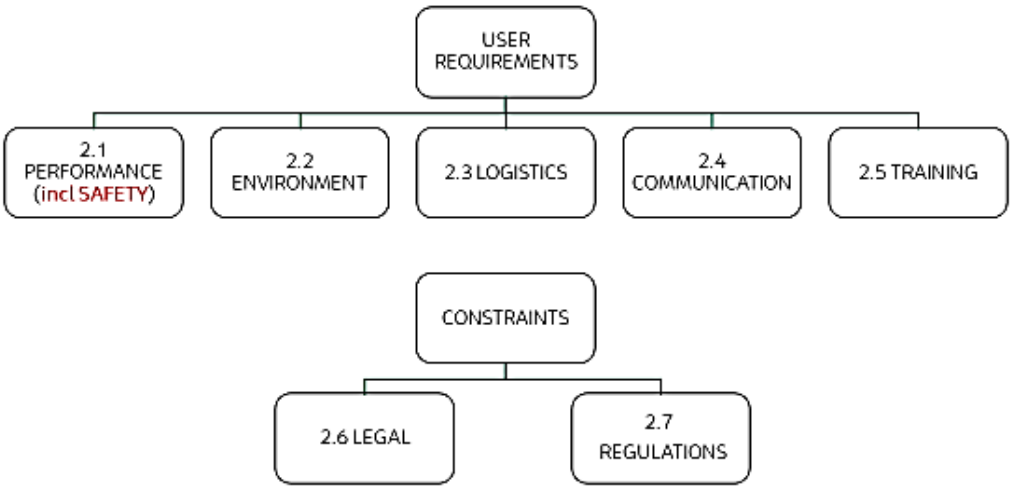


Figure 3 – Example User Requirements Document (URD) Structure

21. **Through Life Safety Perspective**. The SRO **must make sure** that through-life safety requirements, including those associated with disposal/termination, are considered early in the programme. This will help make sure that the capability avoids attributes that

[25] Refer to JSP 912: Human Factors Integration for Defence Systems & Defence Standard 00-251: Human Factors Integration for Defence Systems.

may be difficult to mitigate later in the acquisition lifecycle, such as hazardous materials or stored energy which cannot be recovered, disarmed, or made safe when required. The SRO/User **must make sure** that safety requirements are regularly reviewed though-life to make sure that they remain valid and appropriate.

22. **Measures of Effectiveness (MOE)**. The SRO **must make sure** that MOE of each safety UR provide objective evidence that the requirement has been met. The SRO should not use the requirement to be 'ALARP and Tolerable' as an objective measure, as it is made by the User based on the argument in the SC. The SRO should discuss and agree the safety MOE with the ASC.

23. **Prioritisation**. The SRO **must make sure** safety URs are prioritised alongside other URs. This will make sure that safety is given appropriate consideration and analysis as the programme develops, including within the options selection process and should there be a need to amend or trade URs. Whilst URs can be prioritised and traded, safety risks are required to be ALARP and Tolerable, even if the risk is higher due to a balance against higher levels of capability performance. Legal and regulatory requirements cannot be traded out unless an exemption is available and has been granted.

24. **Legal and Regulatory Requirements**. Legislation includes absolute, prescriptive and proscriptive requirements, as well as those requiring safety risk to be made ALARP. Therefore, safety requirements are likely to include absolute aspects as well as risk-based aspects. The SRO/User **must make sure** that all statutory and regulatory safety requirements, including Defence safety regulations, are identified, assessed and recorded in the appropriate requirements document. The SRO/User **must make sure** that statutory and regulatory safety requirements are actively monitored through-life. This will help make sure that compliance risks due to the emergence of new, or changes to existing, legal and regulatory requirements are identified and managed. The SRO/User should use the Defence Legislation Support Tool (DLST) to assist the identification and monitoring of appliable statutory requirements.

Disapplications, Exemptions or Derogations (DEDs)

25. Health and safety legislation may include DEDs that apply to Defence to enable the delivery of operational capability. Whenever a DED has been incorporated within the legislation then the SRO/User **must make sure** the requirements of the associated Defence safety regulations are followed. Similarly, it might be appropriate to apply for an exemption, waiver or concession from Defence safety policy or regulations if compliance would result in an inability to deliver the required capability. Applications for exemptions should be made on a case-by-case basis and in consultation with MOD Legal Advisers. The SRO/User **must** only apply for exemptions, where available, once all other options have been considered and dismissed. If required, the SRO/User **must** sponsor an application for an exemption to be submitted to the appropriate authority for consideration.

- For legislation, the application should be made in accordance with the requirements of the legislation and JSP 815, Volume 2, Annex B (Exemption Certificate Process). The case for approval is typically considered by the Secretary of State for Defence, although in some cases this may be undertaken on their behalf by the appropriate DSA Regulator, or another Defence appointed body. Guidance in the first instance should be sought from DSA.
- For Defence safety policy, the applications for exemptions should be made to Dir DS. With respect to exemptions from JSP 376, guidance should be sought from

the ASC. For other safety policies, guidance should be sought from DDS Policy Branch.

- For Defence safety regulations, applications for exemptions should be made to the appropriate DSA regulator.

26. Where permission to rely on an exemption from legislation, Defence safety policy or regulations has been sought and granted, the SRO **must make sure** the original requirement is still recorded in the appropriate requirement document. This record should be accompanied by the reason for not meeting that requirement and the rationale for why an exemption was sought.

Test and Evaluation (including Certification)

Key Policy Statement

The SRO/User must make sure that the required safety Test & Evaluation (T&E) activity is included in, and delivered through, the Integrated Test, Evaluation and Acceptance Plan (ITEAP) to provide objective evidence to support the assessment of meeting the programme safety requirements.

27. At the highest level, Test & Evaluation (T&E) aims to provide the SRO with an evidence base that allows them to make well-informed, objective decisions. Broadly speaking, there are 3 reasons to do T&E in Defence: to assure a capability is safe; to assure a capability is contractually compliant (i.e. MOD gets what it wants, and what it paid for); and, to assure that a capability delivers on what the User wants it to do[26].

28. Generally, the nature of T&E activity is inherently hazardous as it may be the first time that the product, service or system has been tested in a real-life situation or the T&E activity itself may be trying to identify working tolerances. Therefore, involvement in these potential high-risk activities in common place in most programmes, and are often undertaken to provide evidence for product, service or system acceptance or the development of the capability.

29. T&E is therefore an important means of providing objective evidence to support the assessment of meeting the programme safety requirements, and is critical to providing evidence to support the pan-DLOD safety argument in the SC. As such, the SRO **must make sure** that the T&E tasks to demonstrate meeting the programme safety requirements are considered early in the programme, alongside other T&E tasks.

30. The ITEAP should be developed alongside the development of the safety requirements set to make sure that the requirements can be demonstrated and then that the appropriate tests are conducted. The SC needs to progressively develop the structured safety argument and feed the supporting evidence requirements into the ITEAP.

Certification

31. Certification is the provision by an independent body of written assurance (a certificate) that a product, service or system in question meets specific requirements[27]. Certification against an appropriate standard can contribute to the justification that a product, service or system has been designed and constructed such that it is safe to operate and therefore support to the case that the residual safety risk has been reduced to ALARP. In addition to equipment certification requirements, there may also be a need to independently certify that other programme elements have been delivered to their specific requirements, such as infrastructure has been built to the appropriate building standards, or that a training course will meet the training requirements.

32. UK legislation requires that certain products, services and systems require certification prior to use. In some circumstances, Defence has a disapplication from these certification requirements. However, in these cases, the Secretary of State's policy requirement requires that Departmental arrangements be maintained that produce outcomes that are, so far as reasonably practicable, at least as good as those maintained by UK legislation[28]. As

[26] QinetiQ: The Fundamentals of Test & Evaluation in Defence.
[27] https://www.iso.org/certification.html.
[28] Secretary of State for Defence's Policy Statement on Health, Safety and Environmental Protection, Paragraph 3.

Defence's independent safety regulator, DSA is responsible for maintaining these certification arrangements through its regulations on behalf of the Defence Safety Function.

33. The SRO **must make sure** to determine which elements of their programme require certification based on statutory and Defence regulatory requirements. Whether the programme will be using Defence and/or statutory certification systems, the SRO **must make sure** that there is liaison with relevant MOD, Other Government Departments (OGD) and external agencies and produce a Certification Strategy that explains the programme through-life approach to certification and identifies certification requirements. Thereafter, the SRO **must make sure** a Certification Plan is produced to meet the programme certification obligations. The SRO **must make sure** the detailed T&E activity required to meet the certification requirements is included in the ITEAP to make sure coherence and make sure there is not duplication of effort.

34. Certification is normally a through-life requirement. Failure to maintain appropriate certification could require the use of the capability to cease. The User **must make sure** that certification is maintained where required, including renewal when certification has been given a defined validity period and re-certification where the terms of the original certification have been changed, for example by a change to the production standard of a product.

Safety Case

Key Policy Statement

The SRO/User must make sure that an evidence-based Safety Case (SC), supporting the argument that a capability is safe, is developed and maintained.

Safety Case

35. The SC is the foundation stone for managing safety risks within the Defence acquisition system. The SC is defined as:

> *A structured argument, supported by a body of evidence that provides a compelling, comprehensible, and valid case that a system[29] is safe for a given application in a given operating environment[30].*

36. Importantly, the SC is through-life, pan-DLOD, and addresses the holistic safety system, including the physical components, operating and maintenance procedures, and human resources organised to deliver the capability. The SC also acts as the structured argument and body of evidence that supports the justification that safety requirements, including the safety KUR(s), are being met as a programme progresses.

37. The SC is required to provide clear, evidence-based argument to show that the safety risks when operating the capability are, and will remain, ALARP and Tolerable in its actual operation: it is not sufficient to show that it could be safe or would be safe in a situation that is unrealistic. A supplier may produce a SC to argue that their solution can be 'operated safely', but that would be qualified with caveats, assumptions, requirements and dependencies that need to be satisfied for the solution to be 'safe in operation'. MOD has legal and regulatory requirements to demonstrate, so far as is reasonably practicable, that its work activities do not expose people to intolerable or unacceptable safety risk.

38. SCs should be proportionate to the safety risks which the capability poses. Understanding the major hazards will help to determine the scale and complexity of the required SC. Therefore, preliminary hazard identification and analysis should be done early in the programme lifecycle to scope the activities and resources needed to build the SC, and then reviewed regularly to make sure that this remains the case throughout the life of the capability.

39. The SRO **must make sure** that the SC development starts at the Pre-Concept Phase, and continually develops throughout the programme to provide evidence to answer the following questions:

- What are the safety requirements of the programme?
- Has the capability been designed, developed, and produced to meet the safety requirements?
- Is the capability being operated to sustain the safety requirements?

40. As such, the SC is a form of risk assessment, developed in advance of using the capability, to demonstrate that residual safety risks are ALARP and Tolerable. The SC

---

[29] *"A combination, with defined boundaries, of elements that are used together in a defined operating environment to perform a given task or achieve a specific purpose. The elements may include personnel, procedures, materials, tools, products, facilities, services and/or data as appropriate"* – Defence Standard 00-056: Safety Management Requirements for Defence Systems.

[30] Further details on the product, service or system elements of a SC are set out in Defence Standard 00-056: Safety Management Requirements for Defence Systems.

then acts as a key component of the risk assessments conducted for specific activity events. The development of the evidence to address the areas above should therefore follow the standard safety risk assessment methodology as detailed in JSP 815, Volume 2, Element 4 (Risk Assessments and Safety Cases).

Safety Case Accountability and Ownership

41. Having identified that the SC is required to fulfil a key function throughout the life of a capability, it follows that there needs to be a clearly identified owner of the SC at each stage of its development. However, due to the nature of Defence procurement and capability development, SC ownership is best conducted through use of Accountable[31]/Responsible[32] relationship terminology as described in the following paragraphs. Unless otherwise stated, SC accountability and ownership should be aligned. An overview of SC accountability and ownership is presented at Annex B.

42. The SRO/User **must make sure** that SC ownership and responsibilities are clearly expressed in the SMP. While the SRO/User may assign responsibility for development and maintenance of the SC, as a whole or in parts, to safety subject matter experts (including contracting to industry), they remain fully accountable for it. In general:

- During the procurement phases, prior to introduction into service, the SRO is accountable for the development of the SC. Early and ongoing engagement and consultation with the proposed User is critical to successful development, growing over time as the programme develops and culminating in endorsement and handover of the SC to the User as the capability enters service.
- The User is accountable for the ownership and maintenance of the SC for the In-Service and Disposal/Termination phases[33].
- Where T&E activity is controlled by MOD, the T&E User is accountable for the production of a separate T&E SC, supported by the SRO and User. The T&E User **must make sure** that the T&E SC demonstrates that a capability is safe for conduct of the planned T&E activity and associated safety risks are reduced to both ALARP and Tolerable. Whilst some elements of the T&E SC and the primary SC are likely to be common, the context for each will be different and the T&E SC scope will be limited to the specific T&E activity.

Safety Case Report

43. The SCR is a summary of the safety argument at a point in time. It captures the key components of the SC, articulating the safety claim, argument and supporting evidence in a clear and concise format. SCRs therefore form a key element of the safety evidence that supports programme key decision points, and the SRO **must make sure** that the SCR is shared with the ASC as part of supporting safety evidence for submission.

---

[31] Accountable – Personably answerable for an activity. Accountability cannot be delegated, unlike responsibility. Managing Successful Programmes (MSP®).

[32] Responsible – Used to describe the individual who has the authority and is expected to deliver a task or activity; responsibility can be delegated. Managing Successful Programmes (MSP®).

[33] Except for submarines, where the User function is conducted by the Defence Nuclear Organisation (DNO). Navy Command (as the User for in-service submarines) is responsible for working with DNO and making sure that they support DNO by handing over ownership of the submarines on removal from service, including ownership of the SC, in a similar way that they received the submarines into service from the SRO on introduction into service.

44. SCRs are required to demonstrate that safety risks associated with capability are expected to be ALARP and Tolerable at the point when the capability enters service and can be maintained as such throughout the expected service life. Once a capability enters service, the SCR is required to demonstrate that safety risks associated with the capability are ALARP and Tolerable. Whilst the contents of a SCR will vary depending on several factors (e.g. the risk and complexity of the programme, stage of the acquisition lifecycle, etc.) the SCR should:

- Include a brief description of the capability, referencing out to the full description contained within the SC.
- Identify the scope of analysis and any supporting evidence used.
- Articulate the safety work that has been undertaken on the programme to date.
- Contain information on assumptions and limitations regarding the safe operation of a capability.
- Incorporate the key elements of the safety argument and references to evidence so that, in principle, it would be possible to access the complete SC, starting from the Report, or counter-evidence where it has been identified.

45. **SCR Accountability and Ownership**. Accountability for, and ownership of, the SCR sits alongside SC accountability and ownership. Therefore:

- The SRO **must** sign and approve SCRs at the key decision points in the procurement phases of the acquisition cycle to accept that the safety argument is sufficiently mature to support the case to move forward to the next acquisition phase.
- At the start of and during the In-Service Phase, the User **must** sign and approve SCRs at appropriate points[34] to accept that the residual safety risks associated with the operation of the capability continue to be ALARP and Tolerable. During the Disposal/Termination Phase (and where unplanned disposal is required (e.g. after a crash/accident, etc.)), the User should sign and approve an SCR to accept that the residual safety risks associated with disposal/termination are ALARP and Tolerable.

[34] See Chapter 3, Paragraph 101.

Supervision and Control Activities

Key Policy Statement

The SRO/User must make sure that the safety risks associated with all activity using the military capability are assessed and mitigation measures are implemented to reduce the residual safety risks to a level that is ALARP and Tolerable.

46. Using the SC as the baseline, the SRO/User **must make sure** that suitable and sufficient risk assessments are completed in accordance with JSP 815, Volume 2, Element 4 (Risk Assessments and Safety Cases) to demonstrate that all the appropriate supervision and control measures are in place and that the residual safety risks have been mitigated to a level that is ALARP and Tolerable.

47. The SRO/User **must make sure** that all activity using the capability is conducted in a safe manner and in accordance with the appropriate instructions.

48. The SRO/T&E User should pay particular attention to supervision and control activities during T&E, where the SC may not have been fully developed and the operating characteristics of the solution may not be fully understood.

Acquisition Safety Assurance and Approvals Decision Support

Key Policy Statements

The SRO/User must make sure that assurance arrangements are put in place that provide confidence that the programme will deliver and maintain a safe military capability.

Dir DS must put in place arrangements to provide the MOD Head Office Approving Authorities with independent analysis and advice of programme safety in support of key programme decision points.

Heads of Defence organisations must make sure arrangements are put in place to provide delegated Approving Authorities with independent analysis and advice of programme safety in support of key programme decision points.

Acquisition Safety Assurance

49. As agreed through the Defence Safety and Environment Committee (DSEC) and MOD 2nd Permanent Under Secretary of State (2PUS) Accounting Officer the DDS should own Defence Safety Policy through the Defence Safety Operating Model; this further clarifies the safety assurance responsibilities to support the SRO and User[35]. This codifies how the Defence safety vision will be assured and the SMS achieved within it.

50. Defence operates the three Lines of Defence (LoD) assurance model for safety. In general, for acquisition safety:

- 1st LoD assurance will normally be provided from within the programme, including the individual elements/projects and at programme level;
- 2nd LoD assurance will normally be provided from outside of the programme. This includes:
    - within the SRO/User's Defence organisation36,
    - within an individual elements/projects Defence organisation37, and
    - within the DDS, with the ASC contributing functional approvals decision support to the AA;
- 3rd LoD assurance will normally be provided by the DSA.

51. In addition to the three LoD assurance model for safety, some programmes may be subject to external assurance through for example the National Audit Office (NAO), the Major Projects Review Group (MPRG) and Infrastructure and Projects Authority (IPA).

52. **Programme Assurance Responsibility**. The SRO/User are responsible for programme assurance arrangements.

- During the procurement phases, the SRO **must make sure** that pan-DLOD safety assurance arrangements are established and undertaken. These arrangements will provide ongoing confidence, and identify areas of risk, in the delivery of a safe capability to the User. As the programme progresses, the User should use the

[35] 20221010-Letter to FSG and FDG HSEP Op Model updates-OS.
[36] e.g. Army Capability Safety Group, RAF Safety Centre, etc.
[37] e.g. DE&S/SDA for the equipment elements of the programme.

assurance generated from these arrangements to support their assessment of programme delivery and, at the appropriate point, the decision to accept the capability into service.

- During the In-Service and Disposal/Termination phases, the User **must make sure** that safety assurance arrangements are maintained and implemented. This will provide confidence that the capability is being operated and disposed of in accordance with the safety requirements and the SC.

53. **Safety Assurance Model (SAM)**. The SRO/User **must make sure** that a SAM is established and implemented as part of the programme's safety management arrangements. The SAM may form part of the Programme SMP. The SAM should demonstrate how safety assurance is delivered across all projects/DLODs and all assurance LoD. The SAM will enable the SRO across the programme to see when safety assurance was last delivered and where there may be safety assurance gaps. Where appropriate, the SRO/User should also consider:

- the provision of safety advice from MOD executive agencies (e.g. Dstl) and external organisations (e.g. IPA).

- using an independent safety assurance provider[38] to enhance the assurance provided by other assurance providers.

Approvals Decision Support

54. In accordance with JSP 655, the SRO is required to establish the approval route in consultation with the Defence Portfolio and Approvals Secretariat (DPAS), and evidence that will be required by the Approvals Decision Support Community, as the programme progresses[39]. The Approvals Decision Support team for a case comprises a variety of disciplines as the programme requires, with either a Head Office or Defence organisation approvals decision support team established depending on the Approving Authority and specific submission to be presented.

55. The ASC is a functional member of the Head Office Approvals Decision Support Community and supports Dir DS in their IAC safety advisor role. Based on the independent analysis of the AA submission and supporting safety evidence provided by the SRO, the ASC

[38] Further information on independent safety assurance can be found within The Institution of Engineering and Technology (IET) factfiles here: https://www.theiet.org/impact-society/factfiles/isa-factfiles/
[39] JSP 655, Part 1, Paragraph 113.

will provide input to the MOD Approvals Decision Support Reports. An overview of the ASC Approvals Decision Support process is at Figure 4.

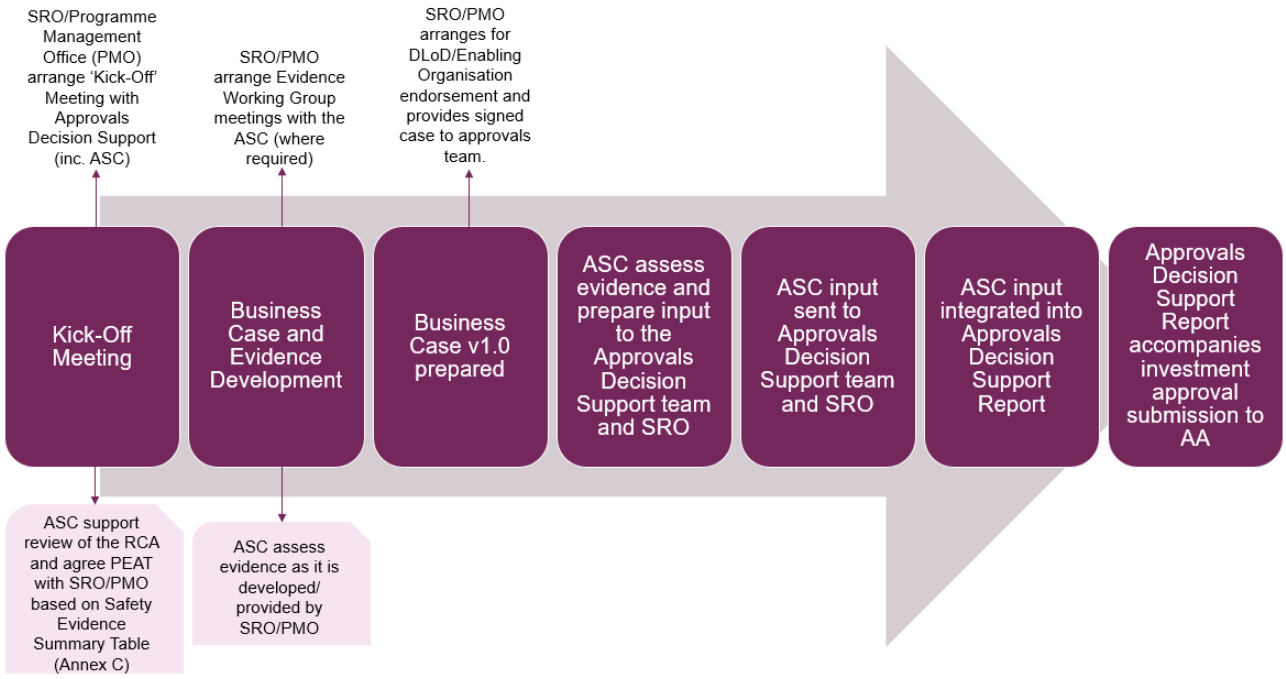


Figure 4 – Overview of the ASC Approvals Decision Support Process

56. **Delegated approvals.** While the ASC will primarily focus on the provision of advice to the IAC, the need for safety approvals decision support is applicable to all capability programmes. Therefore, Heads of Defence organisations **must make sure** that independent safety advice and safety approvals decision support arrangements are established for their delegated AA appropriate to size, complexity and safety risk of those programmes. Also, Heads of Defence organisations **must make sure** that internal governance frameworks take account of safety when considering programmes for submission to the AA at all levels.

57. **Safety Evidence.** The SRO **must make sure** that the ASC is consulted to develop the safety specific lines of enquiry in the Programme Evidence and Assurance Tailoring (PEAT) tool, before agreeing their inclusion in the Programme Evidence and Assurance Plan (PEAP). Lines of enquiry should include the specific safety evidence requirements for each approval stage which are further detailed further in Chapter 3. As part of these lines of enquiry, the programme will be assured by the core artefacts expected through fundamental programme safety governance. A guide to the safety evidence typically required at the end of each phase is detailed within the Safety Evidence Summary Table (SEST) at Annex C. Adequate supporting safety evidence provides confidence that safety has been appropriately managed in the programme to date and plans are in place for that safe management to continue through the subsequent programme phases. However, each programme is different, and the evidence required could be provided in an alternative way. The SRO should therefore engage early with the ASC to tailor the safety approvals decision support requirement and confirm what safety evidence is to be provided in support of each AA submission. Once the requirement has been agreed and included in the PEAP, the SRO **must make sure** that the evidence is provided to the ASC to support the AA submission.

58. **Investment Approvals Submissions.** Safety can only be effectively managed, and safe capability delivered, if it is integrated within all aspects of the programme. The SRO

must demonstrate in their submissions that safety has been adequately addressed across all five cases[40] within the overall BC.

- **Strategic**. The Strategic Case should demonstrate how safety has been considered as part of the overall case for change that has driven the need for the programme.

- **Economic**. The Economic Case should demonstrate how safety will contribute to the net value to society that the programme will bring. This includes factoring in the assessment of safety risks and their associated costs. Further guidance is available in JSP 507.

- **Commercial**. The Commercial Case should show how safety has been included in the commercial deal, including the use of levers and incentives to deliver the required safety outcomes.

- **Financial**. The Financial Case should demonstrate how safety has been incorporated into the overall financial model, including how safety changes might impact on the programme financial position and, similarly, how changes to the programme financial position might impact on safety.

- **Management**. The Management case should safety has been included in the overall programme management and delivery plans.

More detailed guidance is provided for each AA submission in the appropriate section of Chapter 3.

59. **Review Notes.** The ASC will also provide approvals decision support input to the AA where there is a need for the SRO/User to seek approval outside of the standard JSP 655 3-stage BC approval cycle[41] through the submission of a Review Note (RN). The requirement for how safety should be covered within the RN and the supporting safety information will be tailored for each submission. However, the start point should be that any safety implications of the RN recommendations are covered in the submission and the level of supporting safety information will be similar to that for the previous BC submission[42]. The SRO/User should seek advice from ASC as soon as it is identified that a RN submission will be required to agree the supporting safety information requirement.

60. **Information Notes.** Information Notes (IN) may be submitted to the AA for a wide variety of reasons. Although INs through JSP 655 are not subject to formal MOD Approvals Decision Support, unless in exception agreed with the SRO or requested by the AA, the SRO should seek advice from ASC as soon as it is identified that an IN submission will be required to include supporting safety information and assurance.

[40] Strategic, Economic, Commercial, Financial and Management.
[41] Strategic Outline Case (SOC)/Outline Business Case (OBC)/Full Business Case (FBC).
[42] For example, a RN submission during the Assessment Phase will require safety supporting information similar to that required for an OBC submission.

3 Application to the Standard Acquisition Lifecycle Phases

Pre-Concept Phase

Key Policy Statement

During the Pre-Concept Phase, the SRO must make sure that safety is formally considered as a factor when deciding whether and how to proceed with the programme, and as a candidate KUR for high risk and complexity programmes.

1. At the earliest stage of a programme the emphasis is on deciding whether the capability requirement can, in principle, be met sufficiently safely. Initial activities should include identifying stakeholders and consulting with them. This will help gain an understanding of the capability required, interfaces with other capabilities and any constraints on the solution.

Safety Management

2. **Annual Budget Cycle (ABC) Options**. As programmes are initiated from Capability Management Plans and initial funding is being sought, Heads of Defence organisations **must make sure** that safety is explicitly addressed within a programme's ABC Option Approval process to make sure that safety is considered as a factor from the outset of programme initiation.

3. **SRO Appointment Letter**. When appointed, the SRO **must make sure** their Appointment Letter sets out the safety responsibilities of the role. The SRO **must make sure** the Programme Mandate includes the safety assumptions, constraints, boundaries, and dependencies. As the programme develops, the SRO should continually review their Appointment Letter and the Programme Mandate to make sure that they reflect the scope of the programme and the SRO's safety responsibilities.

4. **Programme Management Plan**. In developing the overall Programme Management Plan, the SRO should identify how the various elements/projects of the programme will be delivered. The responsibility for safety should be assigned to a suitable competent individual for each element/project, with the SRO providing oversight of project-level safety. The SRO should pay special attention to safety at the internal interfaces between the elements/projects within their programme and external interfaces with other programmes. A clear understanding of the internal and external programme structure will enable the SRO/User to manage safety across the whole programme. Then, the SRO **must make sure** that a safety section is included within the Programme Management Plan setting out how they propose to manage the safety aspects of the programme and include safety task lines within the Integrated Master Schedule.

5. **Stakeholder Management**. The SRO **must make sure** that key safety stakeholders are included in their overall Stakeholder Map and engagement planning, including the User, the ASC, Delivery Agent(s), DSA Regulators, Statutory Safety Regulators, Certification Bodies and Military Command Safety Management Teams. Where the safety stakeholder community is complex (such as where there are multiple relevant regulatory

bodies), the SRO may consider creating a separate safety stakeholder map and engagement plan, although this approach risks safety becoming separate from core programme stakeholder management and engagement activity. The SRO should make sure that there is early engagement with key safety stakeholders, in particular the User and DSA Regulators. The SRO **must make sure** the ASC is invited to attend programme initiation meetings.

6. **Risk and Complexity Assessment (RCA)**. The SRO **must make sure** that the safety assessment and score rationale are included within the RCA Tool[43]. The SRO should discuss the RCA safety assessment with the ASC. The SRO **must make sure** the safety assessment contained within the RCA Tool is kept up to date and revisited at the start of each phase of the programme lifecycle or where there has been a material change in the programme across any of the DLODs.

7. **Safety Governance**. The SRO **must make sure** that safety governance arrangements are established and maintained to consider programme safety risks and issues, including a programme-level safety risk register and links to element/project-level safety arrangements (such as the Delivery Agent project safety committee or equivalent). While a dedicated programme safety risk forum may be established to consider safety risks and issues in detail, the SRO **must make sure** that key safety risks and issues that may impact the programme alongside other programme risks and issues are identified and managed.

Safety Requirements

8. **Safety Intent**. In the pre-concept stage, the SRO **must make sure** that the safety intent is described through the draft HLC based on the capability concept documents, including the intended safety benefits. Recognising that capability may be met by a wide range of potential solutions, the SRO **must make sure** that the acceptance strategy for potential safety requirements is considered, including identifying the statutory legislation, Defence safety policy and regulations. The SRO should engage with the ASC on the safety requirements. The ASC will provide advice to the relevant ROC.

9. **Safety KURs**. The SRO **must** include safety as one of the candidate KURs for high risk and complexity programmes. The safety KUR may focus on the required safety performance of the capability e.g. the level of safety protection to be provided, or the extent to which particular safety hazards need to be controlled. Alternatively, it may be framed around compliance with the applicable safety legislation, JSP 815, and the underpinning Defence safety policy and regulations. Further advice and guidance on safety KURs is available from the ASC.

Safety Case

10. Different approaches may be taken to the development and maintenance of the SC depending on the solution being procured. For example, the SC is likely to be developed differently if the solution is being acquired as a standalone product or an integrated system, or whether the wider solution includes elements that are being procured through an Off-The-Shelf (OTS) or bespoke development route. During the Pre-Concept Phase, the SRO **must make sure** that a Safety Case Strategy is developed, setting out how the programme will approach the through-life development and management of the SC, and

[43] This assessment provides evidence to support acquisition delivery decision-making, strategic planning, risk management; and should be undertaken alongside the standard risk management practices set out in JSP 892: Risk Management.

provide the evidence required to demonstrate the delivery and maintenance of a safe capability.

Acquisition Safety Assurance and Approvals Decision Support

11. As part of the Programme Management Plan, the SRO **must make sure** that the approach to programme safety assurance is documented, including the initial development of a SAM to be implemented from the Concept Phase.

12. The SRO **must make sure** that safety is included in the Integrated Assurance and Approvals Plan (IAAP). The SRO **must make sure** that the safety evidence lines of enquiry required within PEAP are agree with the ASC. This should be guided by the SEST at Annex C. The ASC should be invited to participate in the Evidence Working Groups.

13. **Strategic Outline Case.** The Strategic Outline Case (SOC) will be submitted to the AA at the end of the Pre-Concept Phase. In the SOC, the SRO **must make sure** that safety has been considered alongside other performance criteria across all five cases within the BC, using the direction and guidance set out in Table 1.

Case	SOC Safety Evidence Requirements
Strategic	HLC include safety requirements, including compliance with legislation, Defence safety policy and regulations. Consideration of safety aspects within relevant Defence Doctrine and the draft CONEMP, including any significant changes from any legacy systems. Information on accidents, incidents and near misses from legacy systems and comparable commercial systems be included where available.
Economic	Consideration of safety within the options appraisal process, including the military capability benefits. Initial options down select analysis if conducted at this point) includes safety considerations within the PCT trade-off.
Commercial	Evidence provided that potential suppliers have the required capability to safely design, produce, support and/or dispose of the elements of the programme for which they may be contracted to.
Financial	Initial cost modelling includes the safety costs and benefits. The ASC should be consulted on safety-related assumptions.
Management	Evidence of how the programme will be managed from a safety perspective, including the governance, safety resources and interfaces. Safety risks and dependencies identified. Consideration given to where exemptions might be required from legislation, Defence safety policy and regulations. Initial schedule modelling should include the planned safety activities.

Table 1 SOC Safety Evidence Requirements

14. **Approvals Decision Support**. Supporting the Head Office Approvals Decision Support Team advice to the AA, the ASC will:

- analyse the SOC and the supporting safety evidence required in the PEAP,
- provide advice on the programme's delivery against the acquisition safety policy requirements; and
- advise in the confidence that the programme will deliver a safe capability.

Concept Phase

Key Policy Statement

During the Concept Phase, the SRO must make sure that safety is included in the user requirement list and the alternative concepts are assessed from a safety risk perspective.

15. At this stage, the solution may be unknown, or understood only as a conceptual outline with a range of viable solutions. Stakeholder engagement will help to identify the safety regulatory or approval regime that will apply to the system when it comes into service, and any specific requirements for safety information which need to be provided. Safety activity should focus on establishing the safety requirements and determining whether the capability requirements can be met without causing unacceptable safety risks to MOD personnel, contractors or members of the public. Where unacceptable safety risks are identified, the SRO **must** consider whether these risks can be eliminated or reduced during the development process and make recommendations in the OBC submission.

Safety Management

16. **SMP**. During the Concept Phase, the SRO **must make sure** that a SMP is developed and implemented, documenting and driving safety across the programme. In addition to implementing the SMP in this phase, the SRO should make sure that the SMP is developed to cover activities during the Assessment Phase and thereafter.

17. **OSA**. The SRO **must** consider the need for an OSA to assess impact of the organisation change resulting from the introduction of the capability and be able to justify a decision that one is not required. If an OSA is required, the SRO **must make sure** that a safety baseline of the current capabilities is completed in conjunction with the User during the Concept Phase. This baseline will be used to assess the safety impact of the proposed change prior to the main investment decision.

Safety Requirements

18. The SRO **must make sure** that the appropriate safety requirements are included in the URD, supporting the safety KUR. The relevant ROC will examine whether the SRO understands the safety drivers in their programme, including the CONEMP and safety implications of any PCT trades. The relevant ROC will analyse whether the URD addresses the safety requirements, including the full DLOD safety implications and dependencies. The ASC will provide safety advice to the relevant ROC.

19. As the URD is developed, the SRO **must make sure** that safety is included within programme assessment methodology to down select to the preferred option.

Test and Evaluation (including Certification)

20. During the Concept Phase, the SRO **must make sure** that the programme T&E Strategy demonstrates the overall approach to T&E to provide the evidence that the programme requirements are being met, including they safety requirements. The T&E Strategy should also identify which elements of the programme will require certification.

Where certification will be required, the SRO **must make sure** that a through-life Certification Strategy is produced in consultation with the relevant Certification Bodies.

Safety Case

21. During the Concept Phase, the SRO **must make sure** that the SC provides evidence that all the safety requirements have been included in the URD, the key safety risks are understood and the safety conclusions of the assessment of the potential capability options have been considered.

22. The SRO should identify, and engage with, the User(s) of the capability during the Concept Phase. The User should be consulted on the capability's safety requirements, interfaces with other capabilities and any constraints on the solution.

23. The SRO should include analysis of accidents, incidents, near misses, and lessons learned from the use of similar capabilities as part of the initial identification of key safety risks that the programme will need to address.

24. **OBC SCR**. In support of the OBC submission, the SRO **must** sign and approve an OBC SCR. The OBC SCR should summarise the safety argument at this point in the programme, and demonstrate that the proposed approach, processes and measures described are likely to support effective ALARP and Tolerable judgments. The SRO **must make sure** that the OBC SCR is shared with the ASC as part of supporting safety evidence for submission.

Supervision and Control Activities

25. Where the Concept phase includes any activity, such as through experimentation or concept demonstration, the SRO **must make sure** that all such activity is supported by a suitable and sufficient risk assessment and that the identified supervision and control activities are implemented. This requirement applies especially when the activity involves using equipment in novel ways and where operator training may be limited. Where the activity is conducted by a contractor in support of a Defence programme, the SRO should make sure that the contractor's risk assessment is suitable and sufficient to minimise indirect reputational risks to Defence.

Acquisition Safety Assurance and Approvals Decision Support

26. As part of the safety management arrangements for the Concept Phase, the SRO **must make sure** that the SAM continues to be developed and implemented.

27. The SRO **must make sure** that the safety evidence lines of enquiry required within PEAP are agreed with the ASC. This should be guided by the SEST at Annex C. The ASC should be invited to participate in the Evidence Working Groups.

28. **Outline Business Case**. The SRO will submit an OBC to the AA at the end of the Concept Phase. In the OBC, the SRO **must make sure** that safety has been used as a factor in the assessment of the range of potential options that will be taken forward into the Assessment Phase. The SRO **must make sure** that safety has been considered alongside other performance criteria across all five cases within the BC, using the direction and guidance set out in Table 2.

Case	OBC Safety Evidence Requirements
Strategic	Safety URs have been identified through appropriate systems analysis and captured within the URD. Safety aspects included within the CONEMP, including any safety constraints and assumptions. Benefits

	Map includes safety aspects and key safety design drivers and standards identified. SC developed to establish that the capability has the potential to be managed safely across all DLODs through its lifecycle.
Economic	The expected safety performance of different design options informs the choice of recommended option, including a ranking of options from the safety perspective.
Commercial	Preliminary engagement with potential suppliers has demonstrated that the safety of the capability will be built into the design and production process. Procurement strategy based on Government-to-Government arrangements (e.g. Foreign Military Sales (FMS), Memorandum of Understanding (MOU), Treaty) recognises the potential for non-compliance with UK safety and environmental legislation (e.g. asbestos, Persistent Organic Pollutants) and the inaccessibility of safety information and assurance evidence.
Financial	Cost modelling should demonstrate that safety risks that may impact the programme have been included in the programme cost envelope.
Management	SMP in place, including explanation of safety delegations. Significant safety risks assessed and quantified. Safety governance established. OSA baseline completed. Key safety stakeholders and their information requirements identified. Safety requirements clear within the T&E Strategy. Relevant Certification Bodies (where available) fully engaged, and Certification Strategy agreed and published. Analysis of accidents, incidents and near misses in legacy systems completed. Initial view of any safety risks that are not tolerable and how they might be mitigated. Schedule modelling should demonstrate that safety risks have been included in the programme schedule.

Table 2 - OBC Safety Evidence Requirements

29. **Approvals Decision Support**. Supporting the Head Office Approvals Decision Support Team advice to the IAC, the ASC will:

- analyse the OBC and the supporting safety evidence required in the PEAP,
- provide advice on the programme's delivery against the acquisition safety policy requirements; and
- advise in the confidence that the programme will deliver a safe capability.

Assessment Phase

Key Policy Statement

During the Assessment Phase, the SRO must make sure that the safety perspective is included in the option assessment and preferred option recommendation.

30. At the Assessment stage, the focus is on deciding how the URD safety objectives can be achieved and, where relevant, on determining which design option provides the safer solution. The expected safety performance of different design options should inform the choice of which option should be recommended. If any option has a fundamental shortcoming that will prevent it meeting legal or policy requirements or being made tolerably safe, then this should be identified early and will prevent that solution being adopted. Separate safety activity is conducted for each of the options, although there will be common material because the functions and environment will be similar.

Safety Management

31. The SRO **must make sure** that the SMP continues to be implemented, including the maintenance of strong safety governance across all DLODs to make sure that the outputs of the Assessment Phase produce a preferred option to deliver a safe capability. In particular, the SRO **must make sure** that the impact on safety is considered during the option assessment and selection activity.

32. The SRO should also make sure that the SMP is developed to cover activities to be undertaken during the Demonstration Phase and thereafter. This should include clear governance, lines of safety responsibility and reporting for T&E activity.

33. **OSA**. Where required, the SRO **must make sure** that the OSA Assessment and Submission phases are completed in conjunction with the User. This will demonstrate that the organisational change associated with the introduction of the new capability into service will not have a detrimental effect on safety. The SRO should make sure the completed OSA is provided as evidence in support of the Full Business Case (FBC) submission.

Safety Requirements

34. During the Assessment Phase, the CONEMP should be developed into the CONUSE. The URD should be refined and developed by the project elements into the SRD. The SRD captures all the detailed system requirements against which their elements of the overall capability will be delivered and against which acceptance will be assessed. The SRO **must make sure** that the SRD includes all the applicable system safety requirements.

35. The relevant ROC will assess whether the safety KURs remain appropriate, that all the DLOD safety implications are understood, and if any additional safety trade-offs are appropriate. The ASC will provide safety advice to the relevant ROC.

36. **Invitation to Tender (ITT)**. The SRO **must make sure** that the safety requirements are incorporated into the tender process, including inclusion in ITT requirements, and appropriate weighting in the tender assessment. Also, the SRO **must make sure** that the

contract includes the programme safety requirements, including compliance with the appropriate safety Defence Standards[44], safety performance indicators and incentives.

37. **Legislative Compliance Assessment (LCA)**. Part of the assessment of options should be the completion of a LCA. The LCA should provide an assessment of whether statutory safety requirements will be met by the preferred option, or whether there may be a need to rely on statutory exemptions. Where this is the case, the SRO **must** formally consider and satisfy themselves that the programme meets the conditions as stated in the appropriate legislation to rely on a statutory exemption before the submission of the FBC for approval.

Test and Evaluation (including Certification)

38. **ITEAP**. A key activity in the Assessment Phase is the development of a full ITEAP. This will capture all T&E demands for the Demonstration Phase to provide the evidence that the capability being supplied will meet the programme requirements. The SRO **must make sure** that all the safety requirements and associated acceptance strategies are included in the ITEAP.

39. **Certification**. Where it has been identified that elements of the programme will require certification, the SRO **must make sure** that a Certification Plan is developed and agreed with the appropriate Certification Bodies.

Safety Case

40. During the Assessment Phase, the SC should focus on the refinement of safety requirements and assessment of the safety performance of the options. Engagement between the SRO and User should grow during this phase, with the User providing input to the SC on areas where options may have significant safety issues that may be difficult to mitigate.

41. The SRO **must make sure** that the safety aspects of each option have been analysed, with evidence available to show how pan-DLOD safety risks, issues and opportunities have been considered.

42. In support of the FBC submission, the SRO **must** sign and approve an FBC SCR, endorsed by the User. In addition to the requirements detailed within Chapter 2, the SCR should include:

- the contribution that safety has made to the options analysis process,
- the evidence that it is feasible for the preferred option being proposed for approval to meet all the safety requirements, and
- the associated processes and measures described are likely to support effective ALARP and Tolerable judgments by the time the capability is introduced into service.

43. **FBC SCR**. The SRO **must make sure** that the FBC SCR is shared with the ASC as part of supporting safety evidence for submission.

Supervision and Control Activities

44. The Assessment Phase may involve potential suppliers providing examples of the solution being proposed for demonstration. In such cases, the SRO **must make sure** that

[44] Including Defence Standard 00-056: Safety Management Requirements for Defence Systems.

all demonstration activity is supported by a suitable and sufficient risk assessment and that the identified supervision and control activities are implemented, noting that the solution is likely to be unfamiliar to MOD personnel.

45. In addition, where practical assessment activity is undertaken by third parties on behalf of the programme, the SRO should seek assurance that this activity has been the subject to a full risk assessment.

Acquisition Safety Assurance and Approvals Decision Support

46. As part of the safety management arrangements for the Assessment Phase, the SRO **must make sure** that the SAM continues to be developed and implemented.

47. The SRO **must make sure** that the safety evidence lines of enquiry required within PEAP are agreed with the ASC. This should be guided by the SEST at Annex C. The ASC should be invited to participate in the Evidence Working Groups.

48. **Full Business Case**. The FBC will be submitted to the AA at the end of the Assessment Phase. The SRO **must make sure** that the FBC demonstrates that the safety requirements, processes and their artefacts have influenced capability design and selection. The SRO **must make sure** that safety has been considered alongside other performance criteria across all five cases within the BC, using the direction and guidance set out in Table 3.

Case	FBC Safety Evidence Requirements
Strategic	Examine the feasibility of achieving the URD safety objectives. Safety aspects included within the CONUSE, including any safety constraints and assumptions. All system safety requirements identified and 'verified' by appropriate design analysis into a mature SRD. Technical solutions under consideration are subject to a safety assessment, and that the strategies for achieving the safety requirements are clearly documented.
Economic	Document the analytic rationale for arriving at preferred approach/solution and show how it achieves the safety requirements.
Commercial	Recommended supplier shown to have proven capability and adequate resources to build and test a safe capability, in a safe manner. Demonstrate that legal issues have been addressed and articulate any remaining legal concerns. Demonstrate that commercial incentives are in place to improve safety.
Financial	Cost and schedule modelling, independently assured by CAAS-AT, should demonstrate that safety risks have been included in risk in costing or risk outside costing and their potential impact on the schedule.
Management	Updated SMP, including measures to eliminate or mitigate significant safety risks. Revisit the safety assumptions and risks across all DLODs and make sure that any remaining safety risks are now actively managed and funded. Demonstrate appropriate DLOD maturity in support of this FBC commitment. Affirm that methods of safety control and governance are functioning appropriately. Demonstrate that safety risks have been assessed including any opportunities for technology insertion. Describe the approach to safety stakeholder management and communications. Define the safety assurance evidence and acceptance criteria. Certification Plan developed and agreed with the Certification Bodies and certification activities included in the ITEAP. Where safety risks are not tolerable what the mitigation plan is, including the delivery confidence.

Table 3 - FBC Safety Evidence Requirements

49. **Approvals Decision Support**. Supporting the Head Office Approvals Decision Support Team advice to the AA, the ASC will:

- analyse the FBC and the supporting safety evidence required in the PEAP,
- provide advice on the programme's delivery against the acquisition safety policy requirements, and
- advise in the confidence that the programme will deliver a safe capability.

Demonstration Phase

Key Policy Statement

During the Demonstration Phase, the SRO must make sure that evidence is obtained to demonstrate that the safety requirements will be met, and safety risks will be reduced to a level that is ALARP and Tolerable when the capability is due to enter service.

50. The bulk of detailed safety evidence is produced at the Demonstration stage, when the safety assessment is used to guide the design process to produce a safer capability. The aim should be to eliminate safety risks through design changes prior to manufacture since this can be achieved more cost-effectively at this stage than later in the programme.

Safety Management

51. The SRO **must make sure** that the SMP is implemented through the Demonstration Phase. Implementation of the SMP is critical given the potential high-risk T&E activity. Trials are often complex and involve joint activity between MOD and contractor personnel. The SRO should consider the production of a specific, joint trials SMP that sits below the overall Programme SMP and is agreed by both MOD and contractor representatives.

52. The SRO should also make sure that the SMP is developed to cover activities to be undertaken during the Manufacture Phase and thereafter.

53. **Concurrent Demonstration and Manufacture Phases**. Where concurrent Demonstration and Manufacture Phases are taking place, the SRO **must make sure** that arrangements are in place to manage any specific safety risks associated with this concurrency. The close engagement with the User during this phase is critical to the development of plans for the smooth handover of the capability as it enters service.

54. **OSA**. Where required, the SRO **must make sure** that the safety mitigations proposed in the OSA are implemented. This is to provide assurance that the introduction of the new capability into service will not have a detrimental effect on safety.

Safety Requirements

55. During the Demonstration Phase, evidence may become available that certain programme requirements will not be able to be met, in part or in full. In such cases, the SRO **must make sure** the impact on safety requirements is considered alongside all other requirements. Where safety requirements need to be amended or removed, the SRO **must make sure** that these decisions are made by the appropriately appointed individuals, as recorded in the URD and SRD, and there is a fully documented justification and decision record.

56. **LCA/Exemptions**. The LCA should continue to be developed during the Demonstration Phase, with evidence collected to demonstrate compliance with legal and regulatory requirements. Where it has been identified that an exemption from legislation should be relied upon, the SRO, supported by the appropriate Delivery Agent(s), **must** prepare and submit an Exemption Case Submission (ECS) to the Secretary of State (SofS) as early as possible after FBC approval, noting that it may take time to gather all of the required information from the solution supplier. This will allow time for SofS to seek

clarification and/or briefing and make a considered decision while reducing the risk to programme delivery and the solution entering service.

Test and Evaluation (including Certification) / Supervision and Control Activities

57. T&E activity forms a key role in demonstrating the achievement of the safety requirements. The SRO **must make sure** that sufficient evidence is gathered during T&E activity as detailed in the ITEAP to demonstrate that all safety requirements will be met.

58. Evidence of meeting requirements can be gathered by a wide range of T&E activity, such as through calculation, simulation, test, inspection, production test and operator trials. The SRO **must make sure** that the safety of the personnel undertaking the T&E activity is considered when deciding the optimum T&E balance reflected in the ITEAP.

59. T&E activity should be designed to be developmental in nature, testing the solution in a controlled but progressive manner. The SRO and T&E User **must make sure** to pay particular attention to activity which are at or beyond the edge of previous activity, checking that the design intention/material state of the solution concerned should not be compromised.

60. **T&E Safety Responsibilities**.

a. Where the T&E activity is controlled by the MOD, the T&E User **must make sure** that there is a separate T&E SC that they own. The T&E SC will exist in parallel to the primary SC owned and developed by the SRO. Although some elements of these SCs are likely to be common, the context for each will be different. The T&E User **must make sure** that the T&E SC demonstrates through claim, explicit argument, and appropriately cited evidence that the residual safety risks associated with the conduct of all anticipated T&E activity have been reduced to both ALARP and Tolerable. The T&E User **must make sure** that the identified supervision and control activities are implemented. In particular, the T&E User should make sure that operators and maintainers understand the ‘safe to operate’ configuration of the capability, which may change during the T&E activity as the solution design matures and because of lessons identified during previous T&E activity.

b. Where T&E activity is controlled by contractors but includes the participation of MOD personnel, the SRO retains a duty of care for those personnel. Therefore, the SRO **must make sure** that the T&E User conducts a risk assessment to make sure that the safety arrangements for participating MOD staff are sufficient before each T&E activity occurs. This risk assessment should include seeking assurance that the contractor has conducted their own suitable and sufficient risk assessment before any MOD personnel are contracted or co-opted for testing, approval or acceptance activities or whenever they assist in operation of a solution prior to its entry into service.

c. Where the T&E activity is conducted solely by contractors, MOD may not have a direct safety responsibility and limited contractual liability but there may still be legal and reputational risks to be considered. The SRO should therefore seek assurance from the contractors that suitable and sufficient safety measures have been put in place to reduce the residual safety risks to ALARP and Tolerable.

61. In addition to providing evidence of meeting the URs, the output of the Demonstration Phase should be an agreed production standard against which further safety activity can be progressed. Evidence for certification should be gathered from testing on this production standard. The SRO **must make sure** that certification evidence from

Demonstration Phase T&E activity remains valid for the production standard and is not compromised by subsequent changes to the design and production standards.

Safety Case

62. Evidence from T&E activity will be critical to supporting the argument put forward in the SC that the capability is 'safe to operate' and can be 'operated safely'. The SRO **must make sure** that SC is continually developed during the Demonstration Phase to contain all the safety evidence, show how the safety targets are being and will be met, and confirm that sufficient evidence is available to support the ALARP and Tolerable judgement.

63. The involvement of the User should continue to grow during the Demonstration Phase as T&E activity provides evidence of the proposed operating and maintenance procedures, providing them with assurance that the capability, will be safe when ready to be introduced into service.

64. **Demonstration SCR**. The SRO should sign and approve a Demonstration Phase SCR to support the case for moving the programme forward to the Manufacture Phase. In addition to the requirements detailed within Chapter 2, the Demonstration Phase SCR should include confirmation that:

- all the required safety evidence has been successfully gathered,
- the safety evidence gathered supports the growing confidence all the safety requirements will be met, and
- the associated processes and measures described are likely to support effective ALARP and Tolerable judgments.

65. The SRO **must make sure** that the Demonstration Phase SCR is shared with the ASC as part of supporting safety evidence if there is a need for a formal submission to the AA.

Acquisition Safety Assurance and Approvals Decision Support

66. As part of the safety management arrangements for the Demonstration Phase, the SRO **must make sure** that the SAM continues to be developed and implemented.

67. While there is not normally a formal AA submission required at the end of the Demonstration Phase, the supporting safety evidence detailed in the SEST at Annex C should provide the SRO with assurance that the programme, from a safety perspective, is ready to move forward to the Manufacture Phase. Independent advice could be provided by the ASC, for which the SRO should engage with the ASC as early as possible.

68. Where a programme requires a formal AA decision to proceed, the SRO **must make sure** that the ASC is engaged to agree the safety evidence required to support the submission. Supporting the Head Office Approvals Decision Support Team advice to the AA, the ASC will:

- provide advice on the programme's delivery against the acquisition safety policy requirements, and
- advise in the confidence that the programme will deliver a safe capability.

Manufacture Phase

Key Policy Statement

During the Manufacture Phase, the SRO must make sure that the capability is delivered to the standards required, and that the User is satisfied on handover that the residual safety risks have been reduced to an ALARP and Tolerable level.

69. In the Manufacture Phase, the emphasis is on making sure that neither the production process nor any design changes compromise safety across any of the programme elements. Many of the safety assessments to date will have been based on assumptions and pre-manufacture testing data. Once the complete system exists, trials are conducted to verify that these assumptions are valid for the deliverable capability. At this stage, the SRO **must make sure** that the necessary supporting arrangements (including logistics, training, etc) are put in place to show that all the programme elements have come together to deliver a capability that is safe to operate before it is allowed into service.

Safety Management

70. While Defence activity during this phase may be more limited, the SRO **must make sure** that the SMP is implemented during the Manufacture phase. The SMP should address solutions delivered to the User and activity conducted to support declaration of the In-Service Date (ISD), be that through a single introduction into service or, more likely, staged capability growth path from an Initial Operating Capability (IOC) to Full Operating Capability (FOC). Where this is the case, the SRO **must make sure** that the User understands the safety position for each stage of delivery, such as limitations on use, specific safety control measures, etc and the growth path from IOC to FOC from a safety perspective.

71. **SRO/User Safety Transfer**. From a safety perspective, the declaration of the ISD is a two-way agreement between the SRO and User, with:

a. The SRO satisfied that the appropriate safety arrangements, including an in-service SMP construct, are in place to make sure safe operation of the solution and that the User understands the residual safety risks, and

b. The User satisfied that the solution provided is ‘safe to operate’, they have the required information and arrangements to make sure that the solution can safely enter service and be ‘operated safely’ and they accept the residual safety risks.

72. As such, the SRO **must make sure** that all information required for safe operation of the solution[45] is prepared and transferred to the User. The SRO **must make sure** that the hand-over to the User occurs in sufficient time for any additional T&E activity required in support of safety risk judgements to be undertaken and demonstrated before IOC. Then the User **must make sure** that the capability safely enters service in accordance with the agreed deployment plan and that all risk control measures are implemented.

[45] Including procurement safety records, operator safety documentation, and so on.

73. A User who is required to be a Duty Holder **must make sure** that they are formally appointed by the appropriate Senior Duty Holder before they assume responsibility for the capability, including endorsement by the appropriate DSA Regulator(s) if required.

Safety Requirements

74. Should there be a need to amend the requirements because of changes during the Manufacture Phase, the SRO **must make sure** that safety impact of these changes is fully evaluated, documented and agreed by the User and, if required, the appropriate Approving Authority.

75. The SRO **must make sure** that the final version of the URD and SRD, including the safety requirements, is handed over to the User to act as the baseline for later developments of the capability as required.

76. **LCA/Exemptions**. The SRO **must make sure** that a LCA is completed prior to the capability entering service to confirm that statutory and regulatory requirements have been met, or that the appropriate exemptions are in place. Where it has been identified that a new exemption from legislation should be relied on, the SRO, supported by the appropriate Delivery Agent(s), **must** prepare and submit an ECS to the SofS as early as possible, noting that the SofS may need time to seek clarification and/or briefing and make a considered decision.

Test and Evaluation (including Certification)

77. The SRO **must make sure** suitable Quality Assurance plans are implemented across all elements of the programme to provide assurance that the solution delivered meets the agreed production standards and therefore meets the URs, including safety requirements.

78. T&E activity during the Manufacture Phase may support acceptance of a solution, with evidence generated to demonstrate that the solution is safe, fit-for-purpose and meets the defined requirements. The SRO **must make sure** that evidence is available to correlate evaluation outcomes against individual safety requirements.

79. **Certification**. Formal certification of the capability should be based on the production standard and configuration handed over to the User, be that for example a final equipment production standard or a final course design. The SRO **must make sure** that all certification activity is completed, and the required certificates issued prior to in-service use.

80. **Limited Certification**. Where it is not possible to meet all the certification requirements, there may be a need to obtain a limited certification with caveats on use. In such cases, The SRO **must make sure** that the User is fully engaged and agrees to these limitations and caveats. Where these limitations are enduring, the URD should be amended to reflect the change of requirement delivered and agreed by the User and, if required, the appropriate Approving Authority. Where they are temporary, the User should make sure before accepting the capability into use that a funded programme of work is in place to remove the limitations and caveats in a timely manner. In some cases, the DSA Regulator or Certifying Body may place a time limit on the limitations and caveats, beyond which the certification may become invalid.

Safety Case

81. Some changes to the solution design during the Manufacture Phase have the potential to have a significant impact on safety as the available mitigation measures are more limited. The SRO **must make sure** that all proposed design changes that could

impact on safety are discussed with the User, subject to a thorough risk assessment before they are agreed, and the outcome of this risk assessment is reflected in the SC.

82. By the point that the capability enters service, The SRO **must make sure** that the SC is sufficiently mature to fully support the safety argument covering all three aspects of the SC: safety requirements, design and manufacture, and operating and maintenance.

83. **ISD SCR**. Prior to declaration of the ISD, the SRO **must make sure** that an ISD SCR is produced. The ISD SCR should summarise the safety evidence to support the argument that the safety risks have been reduced to ALARP and Tolerable. The User **must** sign and approve the ISD SCR to demonstrate acceptance of the SC as the capability enters service. The SRO **must** share the ISD SCR with the ASC as part of supporting safety evidence if there is a need for a formal submission to the AA.

Supervision and Control Activities

84. The SRO remains accountable for the safe use of the capability until it is formally handed over to the User and accepted into service. During this phase, there will be activity in the form of acceptance trials and initial training to support declaration of the ISD. The SRO **must** work closely with the User and **must make sure** that activity is properly risk assessed and that the identified supervision and control activities are implemented so that the safety risks are reduced to ALARP and Tolerable.

Acquisition Safety Assurance and Approvals Decision Support

85. As part of the safety management arrangements for the Manufacture Phase, the SRO **must make sure** that the SAM continues to be implemented.

86. While there is not normally a formal AA submission required at the end of the Manufacture Phase, the supporting safety evidence detailed in the SEST at Annex C should provide the SRO and User with advice that the programme, from a safety perspective, is ready to move forward to the In-Service Phase. Independent advice could be provided by the ASC, for which the SRO should engage as early as possible.

87. Where a programme requires a formal AA decision to proceed, the SRO **must make sure** that the ASC is engaged to agree the safety evidence required to support the submission. Supporting the Head Office Approvals Decision Support Team advice to the AA, the ASC will:

- provide advice on the programme's delivery against the acquisition safety policy requirements, and
- advise in the confidence that the programme will deliver a safe capability.

In-Service Phase

Key Policy Statement

During the In-Service Phase, the User must make sure that the capability is operated in accordance with the safe operating envelope and that the safety risks remain ALARP and Tolerable.

88. The safety emphasis changes when a capability comes into service. Up until that point, safety activities are principally concerned with influencing the design solution across all programme elements/DLODs, and with preparing the necessary arrangements to keep safety performance high when in-service. Once the capability is in service, the focus should be on avoiding harm through implementing the control measures already decided on (e.g. training, safe systems of work, contingency arrangements), monitoring safety performance and learning the lessons from any accidents, incidents or near misses that do happen. The agreed safety risk control measures are required to be correctly implemented, or the expected level of residual safety risk will be exceeded and may not be considered ALARP and Tolerable. Where this is the case, the User **must make sure** that all the practicable control measures to be implemented to bring the safety risks back to an ALARP and Tolerable level are assessed.

Safety Management

89. **SMP**. The User **must make sure** that the required safety management arrangements are put in place for the in-service operation of the capability, including the implementation of safe controls, safety information management and configuration management[46]. There is no requirement to maintain separate safety management arrangements for each capability and the User may decide to wrap several capabilities into a single set of safety management arrangements, including a single SMP. However, the User **must make sure** they can demonstrate how these arrangements apply to each capability and how the individual characteristics of each capability are considered.

90. Throughout the In-Service Phase, and as the capability approaches its expected Out of Service Date (OSD), the User **must make sure** that arrangements are put in place, including a specific SMP, for the safe disposal of the solution. The User **must make sure** these arrangements are agreed in advance with the appropriate disposal agency.

91. **OSA**.

a. Once FOC has been achieved, the User should carry out a final assessment to confirm that the safety risks mitigations identified within the OSA have been implemented and any additional risk mitigations required put in place. Following this final review any further assurance activity will be part of the Defence organisation's routine assurance regime.

b. Where changes are made during the In-Service Phase either to the capability or use of the capability, the User should consider the need to conduct an OSA prior to the change to confirm that safety standards will be at least as good as previously once the change has been implemented.

[46] As per JSP 945: MOD Policy for Configuration Management.

92. **Lessons Learned (L2)**. Key to maintaining a safe capability is the reporting and analysis of accidents, incidents or near misses. The User **must make sure** that robust reporting and L2 processes are implemented such that the safety risks remain ALARP and Tolerable. The User **must make sure** that any changes identified from the L2 process are documented in the SC, communicated to stakeholders, and implemented.

Safety Requirements

93. The User **must make sure** that the URD is maintained as the baseline for the in-service capability. The User **must make sure** that changes to the capability do not result in the safety elements of the user requirement being compromised. These changes could be because of a capability upkeep[47]/update[48], organisational structural change, changes to training delivery, and so on.

94. While the user requirement may not change, the context in which the capability is required to operate may change. The User **must make sure** that such changes (such as legislation, regulation and technology) are monitored to identify their effect on the solution and its safety.

95. **LCA/Exemptions**. The LCA should continue to be reviewed during the In-Service Phase, accounting for the emergence of new, or changes to existing, legislation and regulations. The LCA should also be reviewed where there are changes to the solution and its use, making sure that legal and regulatory compliance is maintained. Where it has been identified that a new exemption from legislation should be relied on, the User, supported by the Delivery Agent(s), **must** prepare and submit an ECS to the SofS as early as possible, noting that the SofS may need time to seek clarification and/or briefing and make a considered decision. During this period the capability should be removed from operation as it will be in non-compliance with statutory requirements.

96. **Capability Upgrade**. If the capability is required to undergo future development and upgrade[49], a tailored version of the acquisition lifecycle should be followed. Further details on how safety should be included in a capability upgrade is to be included in later versions of this JSP.

Test and Evaluation (including Certification)

97. The User **must make sure** that certification is maintained through-life where required. In-service changes to solutions through modification may require the solution to undergo full or partial recertification. The User should seek advice from the DSA Regulator or Certification Body in the first instance. Continuing to use a solution that should have, but has not, undergone recertification may mean that the use is prohibited and could compromise the integrity of the SC.

98. **Limited Certification**. Where a capability has entered service with limited certification and caveats on its use that restrict the capability from meeting the full User Requirement, the User **must make sure** that the agreed funded programme of work to remove the limitations and caveats is implemented. Where this is not possible, or where a

[47] An upkeep project is one which seeks and results in renewal, continuation, or extension of an existing capability without resulting in additional functionality or material improvement to a capability (SMART Approvals).
[48] An update project is one which seeks to and results in renewal, continuation, or extension of an existing capability, and although it does not necessarily seek it, results in additional functionality or material improvement to a capability (SMART Approvals).
[49] An upgrade project is defined as one that seeks and results in a material improvement to a capability (SMART Approvals).

time limit imposed on the partial certification is due to expire, the User **must make sure** this is declared to the relevant Certification Body or Bodies and that the limitations and caveats on use are enduring or will not be removed. The Certification Body or Bodies will then review the certification and decide whether the capability can continue long-term use with these limitations and caveats and may issue amended certificates accordingly.

Safety Case

99. At the point that the capability enters service, the SC is required to present a claim, supported through explicit argument and appropriately cited evidence, which demonstrates that the capability is safe for the conduct of operations and that the associated safety risk is reduced to both ALARP and Tolerable.

100. The User **must make sure** that the SC is maintained throughout the in-service life of the capability, conducting periodic safety reviews to provide assurance that the safety claims, argument and supporting evidence remain valid and that the residual safety risks remain ALARP and Tolerable. The User should determine the intervals between periodic safety reviews, and record it in the SMP, based on the level of safety risk associated with the capability but should not be longer than every 2 years. This periodic safety review should include production, signature and approval of an In-Service SCR.

101. **SC Reviews**. In addition to the periodic safety review of the SC, there will be other occasions where the User **must make sure** that a safety review is initiated including, but are not limited to:

- A change in the operating context;
- In-service design changes, for example to address obsolescence or where the in-service configuration has moved away from that represented in the SC;
- Changes arising from any contributing DLOD;
- Transfer of the solution to a different operating authority;
- Changes to relevant legislation, regulations, policy or standards;
- Material changes to the safety argument;
- Major change to Statement of Operating Intent and Usage;
- A significant, continuing safety concern or deviations between actual performance and design intent;
- Post an accident, major incident or prior to return to service;
- Recognition of a new condition of higher-technical merit and/or higher-risk activity;
- Adoption of a new technology and/or technique as recognised good practice by the wider industry;
- Plans to change the OSD of the capability.

102. On such occasions, the User **must make sure** that a pan-DLOD safety review of the change is conducted to consider whether any new control measures or changes to existing control measures (including changes to the design of the solution as well as how the solution is used) are required for the residual safety risk position to remain ALARP and Tolerable. Once the safety review has been completed, the User **must make sure** the SC is updated and **must** sign and approve a SCR that summarises the revised safety argument. The User **must make sure** that the changes are not introduced until the arrangements are put in place that support a judgement that the residual safety risks are ALARP and Tolerable. In some cases, the User may have to consider temporary restrictions on the use of the capability while changes to the safety arrangements are implemented.

103. **OSD SCR**. Prior to OSD, The User should produce, sign and approve an OSD SCR to demonstrate that arrangements are in place for the safe disposal/termination of the capability, including the main equipment platforms and any supporting systems (e.g. simulators) and spare parts. The User **must make sure** the OSD SCR is shared with the ASC as part of supporting safety evidence if there is a need for a formal submission to the AA.

Supervision and Control Activities

104. Throughout the In-Service Phase, the User **must make sure** that the capability is operated within the safe operating envelope as described in the SC, properly risk assessed for each specific event and that the identified supervision and control activities are implemented.

105. Where there is a need to temporarily operate outside of the SC-described safe operating envelope (such as on operations), the User **must make sure** that the appropriate risk assessment is carried out and that ownership of that risk is accepted at the appropriate level[50]. Should there be a permanent requirement to operate outside of the safe operating envelope defined by the SC, the User **must** commission a full review of the SC and put in place enduring arrangements that support a judgement that the residual safety risks are ALARP and Tolerable for the new operating envelope (see para 101).

Acquisition Safety Assurance and Approvals Decision Support

106. As part of the safety management arrangements for the in-service operation of the capability, the User **must make sure** that an approach to safety assurance is formulated, including the development of a SAM to be implemented from the In-Service Phase.

107. While there is not normally a formal AA submission required at the end of the In-Service Phase, the supporting safety evidence detailed in the SEST at Annex C should provide the User with assurance that the programme, from a safety perspective, is ready to move forward to the Disposal/Termination Phase. Independent safety advice could be provided by the ASC, for which the User should engage with the ASC as early as possible.

108. Where a programme does require a formal AA decision to proceed, the User **must make sure** that the ASC is engaged to agree the safety evidence required to support the submission. Supporting the Head Office Approvals Decision Support Team advice to the AA, the ASC will:

- provide advice on the programme's delivery against the acquisition safety policy requirements, and
- advise in the confidence that the programme has considered safety as part of its disposal/termination plans.

[50] As per JSP 815, Volume 1, Element 4, Expectation 4.3.

Disposal/Termination Phase

Key Policy Statement

During the Disposal/Termination Phase, the User must make sure that the capability is disposed of in a safe manner.

109. At the end of a capability's life, MOD has a duty to make sure that the capability is disposed of safely. Planning for disposal/termination should begin at an early stage of a programme so that the design can be influenced for safe disposal/termination, for example by eliminating materials that are hazardous to dispose of and by removing or reducing safety hazards that may arise during dismantling. Disposal/termination activities include through-life disposal as well as end-of-life disposal. So safe disposal is required to be considered early for prototypes, test articles, consumables, and where unplanned disposal is required (e.g. after a crash/accident, etc.), which may occur well before the Disposal/Termination Phase. Disposal can be via a number of different routes, including sales, gifting and dismantling. The plan for end-of-life disposal/termination should be refined and updated as the capability is modified and as legislation or policy requirements change.

110. Specific disposal arrangements may occur that require appropriate designation of accountability and responsibility. The User is normally accountable for overseeing this phase, supported by the appropriate disposal agencies (refer to footnote 33).

Safety Management

111. Prior to the declaration of OSD, the User **must make sure** that arrangements are put in place, including a specific SMP, for the safe disposal of the capability. The User **must make sure** these arrangements are agreed in advance with the appropriate disposal agency.

112. During the Disposal/Termination Phase, the User **must make sure** that the requirements of the SMP are followed.

113. **Retention of Records**. Following disposal/termination, the User **must make sure** that through life programme safety documentation is properly archived and retained beyond the life of the system in accordance with JSP 441, JSP 375, Volume 1, Chapter 39 and any relevant Defence safety regulations.

Safety Requirements

114. Disposal/termination safety requirements should have been considered early in the capability's lifecycle. However, given the long life of some Defence capabilities, some of these requirements may have changed over time. The User, working with the disposal agencies, **must make sure** that the disposal/termination safety requirements are reviewed to make sure they remain valid.

115. The User **must make sure** that the disposal agent (e.g. Defence Equipment Sales Authority (DESA)) is informed of the relevant safety issues, prior to their joint agreement as to the best contractual route for disposal. For instance, this could include information about hazardous materials contained in the capability, or legal constraints on its use or disposal.

116. If elements of the capability are sold or given to another owner rather than being scrapped, then MOD is taking the role of supplier. As a supplier, MOD has legal duties to make sure that these elements comply with legislation, are designed and produced to be 'safe to operate' and are supported by suitable information to support their safe operation, maintenance and disposal. The User should make sure that capability elements are sold in a condition that would be considered acceptable for continued use. Where this is not the case, the User **must make sure** that the new owner is made aware of the condition prior to the decision to purchase.

117. **Exemptions**. Where Defence capability has been operated whilst relying on exemptions in legislation, those exemptions may not be available for non-Defence uses. The User, through the disposal agencies, **must make sure** that potential new owners of the capability elements are made fully aware of the legislative framework, including exemptions, under which the capability has been operating prior to a decision to purchase.

Test and Evaluation (including Certification)

118. The User **must make sure** that certification requirements for the safe disposal of solutions and waste are identified and completed. Disposing of a solution or waste without the appropriate safe disposal certification may be illegal.

Safety Case

119. During the Disposal/Termination Phase, the focus of the SC is to make sure that there is an evidence base to be able to demonstrate that the capability will be disposed of safely. The User **must make sure** that the SC is maintained throughout the Disposal/Termination Phase for capability elements sold for scrap as well as for those sold or transferred on loan for further use. In cases of loan or continuing use, the User **must make sure** that effort is focused on confirming their contractual and legal obligations for safety to minimise MOD's liability for subsequent claims for compensation. Transfers to museums or for display should be considered as a change of use and (potentially) change of operating authority, and the SC should be reviewed and, if necessary, transferred to the new owner.

120. **Disposal/Termination SCR**. Prior to final disposal/termination, the User should produce, sign and approve a Disposal/Termination SCR to summarise the evidence that the capability will be disposed of safely. The User **must make sure** the Disposal/Termination SCR is shared with the ASC if required.

Supervision and Control Activities

121. The User remains accountable for the safe operation of the capability until it is formally disposed of. The User, working closely with Delivery Agent(s), including the disposal agency, **must make sure** that all disposal activities are supported by a suitable and sufficient risk assessment and that the identified supervision and control activities are implemented.

Acquisition Safety Assurance and Approvals Decision Support

122. As part of the safety management arrangements for the Disposal/Termination Phase, the User **must make sure** that the SAM continues to be implemented.

123. While there is not normally a formal AA submission required during the Disposal/Termination Phase, the supporting safety evidence detailed in the SEST at Annex C should provide the User with assurance that the programme, from a safety

perspective, is being appropriately managed. Independent safety analysis and advice could be provided by the ASC, for which the User should engage as early as possible.

Annex A

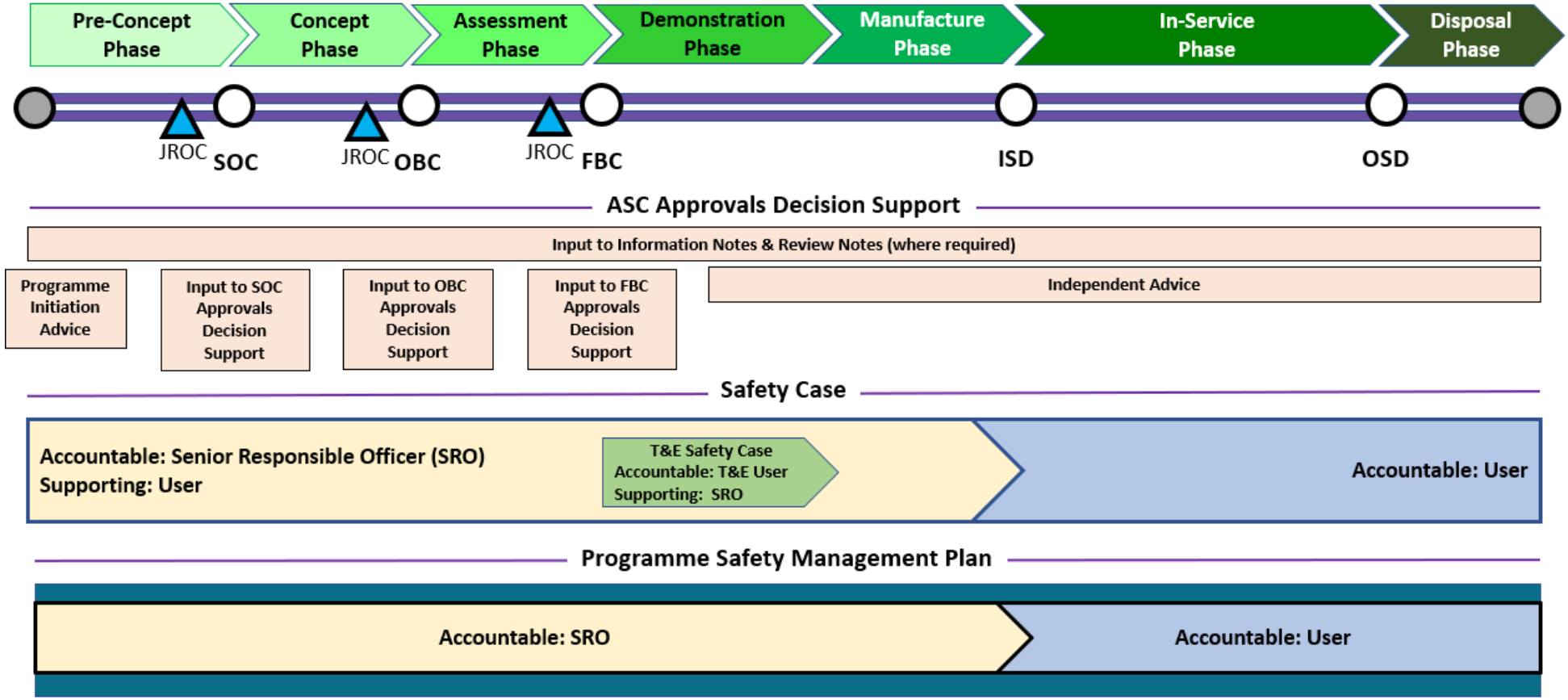
List of Abbreviations

2PUS	2nd Permanent Under Secretary
AA	Approving Authority
ABC	Annual Budget Cycle
ALARP	As Low As Reasonably Practicable
ASC	Acquisition Safety Cell (in the DDS)
BC	Business Case
CAAS-AT	Cost Assurance and Analysis Service Approvals Team
CADMID/T	Concept, Assessment, Demonstration, Manufacture, In-Service, Disposal/Termination
CASP	Command Acquisition Support Plan
CONEMP	Concept of Employment
CONUSE	Concept of Use
COO	Chief Operating Officer
DDS	Directorate of Defence Safety (Policy, Profession & Function)
DED	Disapplication, Exemption and Derogation
DE&S	Defence Equipment & Support
DESA	Defence Equipment Sales Authority
DIO	Defence Infrastructure Organisation
Dir DS	Director of Defence Safety
DLOD	Defence Lines of Development
DLST	Defence Legislation Support Tool
DNO	Defence Nuclear Organisation
DMPP	Defence Major Projects Portfolio
DPAS	Defence Portfolio and Approvals Secretariat
DSA	Defence Safety Authority
DSEC	Defence Safety and Environmental Committee
ECS	Exemption Case Submission
FBC	Full Business Case
FDG	(Safety) Functional Delivery Group
FMS	Foreign Military Sales
FOC	Full Operating Capability
FSG	(Safety) Functional Steering Group
HLC	High-Level Characteristics
HS&EP	Health, Safety and Environmental Protection
HSE	Health and Safety Executive
I&E	Innovation & Experimentation
IAAP	Integrated Assurance and Approvals Plan
IAC	Investment Approvals Committee
IAC(N)	Investment Approvals Committee (Nuclear)
IET	The Institution of Engineering and Technology
IN	Information Note
IOC	Initial Operating Capability
IPA	Infrastructure and Projects Authority
ISD	In-Service Date
ITEAP	Integrated Test, Evaluation and Acceptance Plan
ITT	Invitation to Tender

JROC	Joint Requirements Oversight Committee
JSP	Joint Service Publication
KUR	Key User Requirement
L2	Lessons Learned
LCA	Legislative Compliance Assessment
LoD	(Assurance) Lines of Defence
MOD	Ministry of Defence
MOE	Measure of Effectiveness
MOU	Memorandum of Understanding
MPRG	Major Projects Review Group
NAO	National Audit Office
OBC	Outline Business Case
OGD	Other Government Department
OSA	Organisational Safety Assessment
OSD	Out of Service Date
OTS	Off-The-Shelf
PCT	Performance, Cost and Time
PEAP	Programme Evidence and Assurance Plan
PEAT	Programme Evidence and Assurance Tailoring
PMO	Programme Management Office
RCA	Risk and Complexity Assessment
RN	Review Note
ROC	Requirement Oversight Committee
SAM	Safety Assurance Model
SC	Safety Case
SCR	Safety Case Report
SDA	Submarine Delivery Agency
SEST	Safety Evidence Summary Table (Annex C)
SMART	Specific, Measurable, Achievable, Relevant and Timed
SMP	Safety Management Plan
SMS	Safety Management System
SOC	Strategic Outline Case
SofS	Secretary of State
SRD	Systems Requirement Document
SRO	Senior Responsible Owner
SSUN	Single Statement of User Need
SQEP	Suitably Qualified and Experienced Personnel
T&E	Test and Evaluation
TEPIDOIL	Training, Equipment, Personnel, Information, Concepts & Doctrine, Organisation, Infrastructure, and Logistics
UR	User Requirement
URD	User Requirements Document

Annex B

Programme Acquisition Safety Overview



The scope of the ASC approvals decision support is primarily focused on centrally approved, high risk & complexity programmes, which require investment approval by the Investment Approval Committee (IAC). Heads of Defence Organisations must make sure that delegated Approving Authorities are provided with equivalent acquisition safety advice.

Annex C

Safety Evidence Summary Table

This table acts as an artefact guide for SROs and Users. Director of Acquisition and Programme Delivery PEAT Lines of Enquiry will confirm specific evidence requirements for each formal JSP 655 submission stage.

SRO User

SOC OBC FBC

	Pre-Concept	Concept	Assessment	Demonstration	Manufacture	In-Service	Disposal
Business Case	• Safety in ABC Option • Safety in SOC	• Safety in OBC	• Safety in FBC	• Safety in RN/IN (where required)	• Safety in RN/IN (where required)	• Safety in RN/IN (where required)	• Safety in RN/IN (where required)
Safety Management	• Safety in SRO Appointment Letter and Programme Mandate • Safety in Programme Management Plan • Safety in Programme Risk Register • Safety in IAAP	• Programme SMP • Updated Programme Risk Register • OSA Baseline	• Updated Programme SMP • Updated Programme Risk Register • Completed OSA	• Updated Programme SMP • Updated Programme Risk Register	• Updated Programme SMP • Updated Programme Risk Register • Duty Holder(s) endorsed by DSA Regulators (where required)	• Updated Programme SMP • Updated Programme Risk Register • Reports on Safety Incidents and Accidents	• Disposal Safety Management Plan • Archived Safety Documentation
Safety Requirements	• Safety considered in HLC and as a mandatory KUR • Safety in Options Long List Down Select Analysis • Potential Safety Exemptions identified	• Safety Requirements KUR in the URD • Safety in the SRD • Safety Exemptions Updated	• Safety Requirements in the URD and SRD • Initial LCA • Safety Section in Tender and Contract processes • Safety Exemptions Updated	• Updated URD/SRD • Updated LCA • Safety Exemptions Updated	• Updated URD/SRD • Completed LCA • Exemption Certificates (where required)	• Updated LCA	
Test & Evaluation (inc. Certification)		• Test & Evaluation/ Certification Strategy	• Safety in the ITEAP/ Certification Plan	• Updated Certification Plan	• Certificates	• Updated certificates	• Safe disposal certificates (where required)
Safety Case	• Safety Case Strategy • SOC Safety Case Report	• OBC Safety Case Report • User consultation	• FBC Safety Case Report • User consultation	• Safety Case Report • User consultation	• ISD Safety Case Report • User acceptance	• In-service Safety Case Report(s) • OSD Safety Case Report	• Disposal Safety Case Report
Programme Safety Assurance	• Programme Safety Assurance Model • DSA Assurance (3LOD) • External Assurance (IPA/MPRG/NAO)	• Programme Safety Assurance Model • DSA Assurance (3LOD) • External Assurance (IPA/MPRG/NAO)	• Programme Safety Assurance Model • DSA Assurance (3LOD) • External Assurance (IPA/MPRG/NAO)	• Programme Safety Assurance Model • DSA Assurance (3LOD) • External Assurance (IPA/MPRG/NAO)	• Programme Safety Assurance Model • DSA Assurance (3LOD) • External Assurance (IPA/MPRG/NAO)	• Programme Safety Assurance Model • DSA Assurance (3LOD) • External Assurance (IPA/MPRG/NAO)	• Programme Safety Assurance Model • DSA Assurance (3LOD) • External Assurance (IPA/MPRG/NAO)