SHIPS OPERATING CENTRES' SAFETY & ENVIRONMENTAL PROTECTION ORGANISATION AND ARRANGEMENTS STATEMENT

Ministry of Defence

de&s

LEAFLET 5

SHIPS OPERATING CENTRES'		
END-TO-END SAFETY RISK MANAGEMENT PROCESS		
Sponsor: **DES Ships Eng-SEP-TL**	Issue: **Issue 3**	Date of Issue: **October 2020**
Author: **DES Ships Eng-SEP2**	Verified: **DES Ships Eng-SEP-TL**	Approved: **DES Ships Eng-SEP-TL**

Document History

Issue	Date	Version Comments
1.1	September 2014	
2	June 2017	Updated to include all aspects of the risk management process, along with new material on Hazard Log Rationalistion and use of the eCassandra Hazard Management Tool.
3	October 2020	Updated to reflect: changes to the Navy Command Safety and Environmental Management System; implementation of the DE&S Acquisition Safety Project (ASP); removal of the legacy SHIPS Risk Maturity Descriptors (and use of the term ATRA) and adoption of the eCassandra Accident Descriptors; minor updates to the Risk Classification Matrix; removal of the eCassandra User Guide (relocated to a SEP Technical Note).

Contents

1. Introduction

1.1. The aim of this Leaflet is to ensure that SHIPS OCs' Safety Authorities adopt a coherent, consistent and proportionate approach when managing hazards and risks on behalf of Duty Holders and other Accountable Persons. This Leaflet shall be applied by all SHIPS OC Safety Authorities, including the SALMO team, noting that they will likely be acting as both Hazard Manager and Risk Owner for the high hazard activities they undertake.

1.2. Within this Leaflet, the End-to-End Safety Risk Management Process is laid out in six stages, and there is also supporting guidance on two related activities: Hazard and Risk Management Planning and Hazard Log Management.

1.3. This Leaflet is designed to be used in conjunction with the following key documents:

1.3.1. SEP Technical Note on *"The Use of eCassandra and Reporting".*

1.3.2. DE&S Safety and Environmental Protection Leaflet 02/2011 - "ALARP in a Military Equipment Capability Context";

1.3.3. DE&S Safety and Environmental Protection Leaflet 03/2011 - "Equipment Safety and Environmental Protection (SEP) Risk Referral";

1.3.4. DE&S Safety and Environmental Protection Leaflet 14/2019 - "System Safety Risk Management";

1.3.5. The DE&S Project Oriented Safety Management System (POSMS).

1.4. Further, this Leaflet does not contradict or duplicate generic DE&S policy, processes or guidance, rather it is intended to supplement these with domain specific information to ensure coherence with wider Defence Maritime Regulator (DMR) and Duty Holder/Accountable Person policy, direction and guidance.

1.5. It is important to emphasise that effective implementation of this End-to-End Safety Risk Management Process requires the application of professional judgement and experience, both in terms of safety management and the Equipments/Systems/Platforms under consideration, i.e. it is not intended to be a substitute for competence.

2. Overview

2.1. This End-to-End Risk Management Process comprises the following stages:

2.1.1. Stage 1 - Hazard Identification;

2.1.2. Stage 2 - Risk Analysis and Assessment;

2.1.3. Stage 3 - Generating Options for Risk Control;

2.1.4. Stage 4 - Implementing Risk Control Measures;

2.1.5. Stage 5 - Risk Acceptance;

2.1.6. Stage 6 - Risk Review.

2.2. In addition to this, there are two key supporting activities:

2.2.1. Hazard and Risk Management Planning – to ensure that the above activities are undertaken within a clearly bounded scope.

2.2.2. Hazard Log Management – to ensure that the inputs and outputs from the above activities are captured and managed in a coherent fashion.

2.3. The overall process is illustrated at Figure 1 below and the principles underpinning each of the steps are discussed in more detail within each section.

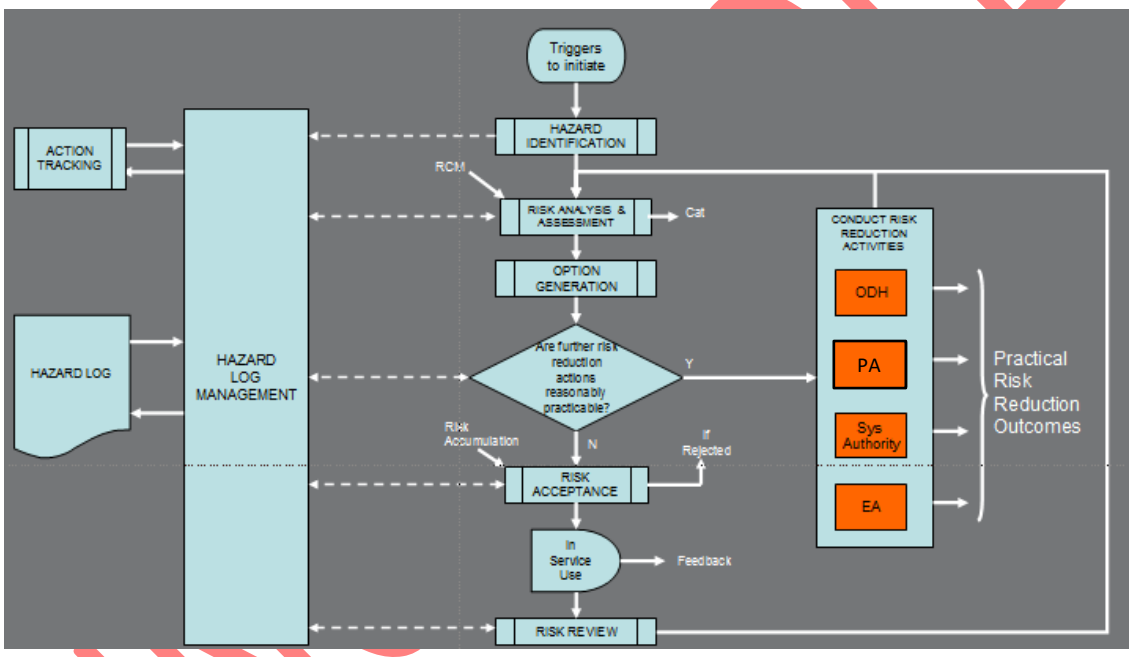


Figure 1 – End-to-End Safety Risk Management Process

3. The Bow-Tie Diagram

3.1. Bow-Tie diagrams provide a graphical representation of the relationship between the various aspects of risk management. They depict the relationship between:

3.1.1. Causes

3.1.2. Preventative safety measures (Safeguards)

3.1.3. Hazard (HLH)

3.1.4. Protective safety measures (Mitigations)

3.1.5. Consequences

3.2. An advantage of adopting the Bow-Tie approach is that it is an extremely powerful representation of the various aspects of risk that can be readily understood at all levels in an organisation. A generic example of the Bow-Tie approach is illustrated in Figure 2 below.

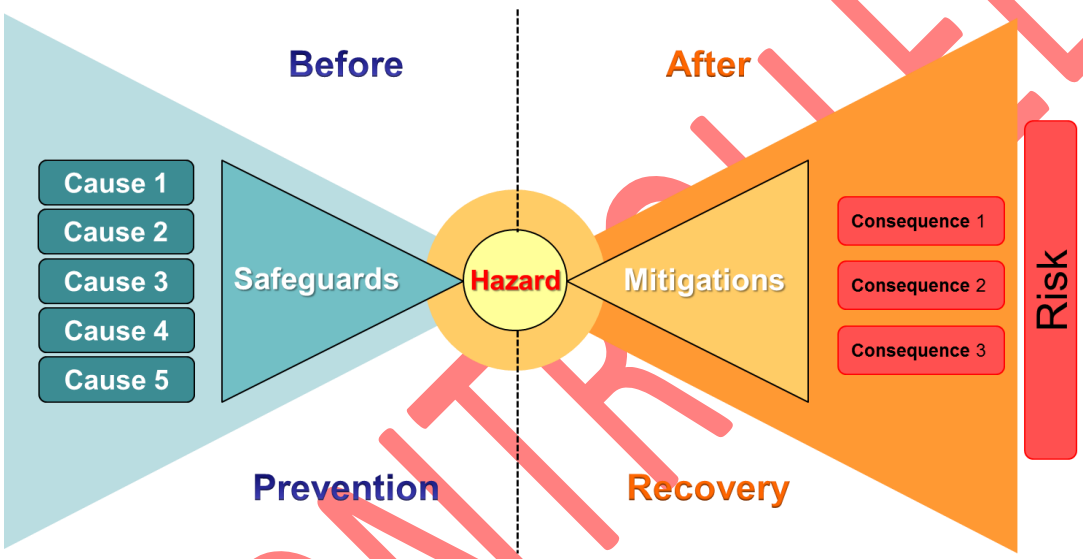


Figure 2 - Bow-Tie Diagram

3.3. The above diagram is included at each section of this document, with the aspects being considered by each stage in the process highlighted via a red box.

4. Key Principles and Responsibilities

KEY RELATED DOCUMENTS

- The Navy Command Duty Holder construct and Risk Management arrangements are described in BRd 10 – Navy Command Safety and Environmental Management Systems, accessible via the Navy Safety Centre web site.
- DE&S guidance on Safety Committees is contained within POSMS Safety Management Procedure SMP02.
- DE&S guidance on Hazard Logs is contained within POSMS Safety Management Procedure SMP11.

4.1. Risk Ownership

4.1.1. All safety risks are owned by an Accountable Person with direct responsibility for the activities generating that Risk.

4.1.2. The underlying principle for Risk ownership across the Front Line Commands is the universal Duty of Care, which stems from statute and is aligned with the Chain of Command. However, where complex military activities present a credible and reasonably foreseeable Risk to Life (RtL)[1], TLBs are required to implement enhanced safety management arrangements through a Duty Holding construct which overlays a higher level of assurance and risk escalation. Accordingly, the Royal Navy's[2] policy for ownership of RtL by formally appointed Duty Holders and other Accountable Persons is as follows:

Class	Risk Owner (Minimum)
A	First Sea Lord (1SL)/Chief of the Naval Staff (CNS) (or as SDH)
B	2* Accountable Person (or as ODH)
C	OF5/1* Accountable Person (or as DDH)
D	Commanding Officer (CO)/Head of Department (HoD)/Head of Establishment (HoE) Accountable Person

4.1.3. Risk owners are ultimately accountable for accepting Risks or formally defining the criteria by which others may accept Risks on their behalf[3], and arrangement for such must be clearly defined within Safety and Environmental Management Plans (SEMPs).

4.2. Hazard Management

4.2.1. All Hazards shall have a nominated Hazard Manager. Typically, Hazard Managers will be senior Engineering/Technical specialists within Platform/System/Equipment Authorities, with a sound knowledge of the engineering and operational use of an Equipment/System/Platform to which the Hazards and Risks under their area of responsibility relate. Hazard Managers are responsible for ensuring that:

4.2.1.1. All available means are taken to identify Hazards and their related Risks;

4.2.1.2. SQEP Panels are convened with suitable membership for the Hazards and Risks under consideration;

4.2.1.3. A full range of options for risk reduction are properly assessed;

4.2.1.4. Recommendations are provided to Risk Owner(s) on risk reduction options as applicable;

4.2.1.5. Effort to reduce risk is suitably prioritised;

4.2.1.6. ALARP Statements are developed, documented and maintained for <u>all</u> Risks;

[1] In the context of this Leaflet, Risk to Life includes those risks where the Consequence Definition from the SHIPS Common Risk Classification Matrix is Major or worse.
[2] Duty Holding arrangements vary across the TLBs, and where PAs/EAs support non-Maritime Users they may need to tailor their risk management arrangements accordingly.
[3] Risks may only be accepted by a suitably empowered representative of the Risk Owner.

4.2.1.7. Actions to maintain the ALARP status and reduce risk are progressed in a timely manner with the ALARP status reassessed or issues escalated;

4.2.2. Hazard Managers in the SHIPS OCs making ALARP recommendations to Duty Holders or other Accountable Persons shall hold an appropriate Letter of Safety Delegation and associated Assignment Specification in accordance with Leaflet 14 of the SHIPS OCs' S&EP O&A Statement.

4.3. Hazard Log Coordinators

4.3.1. All Hazards and Risks shall be managed through a suitable Hazard Log Tool[4]. It is highly recommended that a Hazard Log Coordinator be appointed, with responsibility for:

4.3.1.1. Sole administration for the efficient running of the Hazard Log;

4.3.1.2. Supporting Hazard Managers in marshalling Hazards and Risks for their review/decision;

4.3.1.3. Recording the results of Hazard and Risk management decisions;

4.3.1.4. Monitoring actions on behalf of Hazard Managers;

4.3.1.5. Ensuring that due process is followed in making changes to Hazard Log entries;

4.3.1.6. Initiating the routine review of ALARP risks according to Classification and time from last review.

4.3.2. Hazard Logs should be visible to all relevant stakeholders, and as a minimum this should include Risk Owners and/or their empowered representatives, Hazard Managers and those responsible for validating the implemention of Risk Control Measures.

4.4. Platform Safety and Environmental Committees

4.4.1. For each Platform Class[5], a Platform Safety and Environmental Committee (PSEC)[6] shall be formed, with members responsible for:

4.4.1.1. Reviewing risks referred by a SQEP Panel;

4.4.1.2. Presenting a constructive challenge such that risk control measures are robust, clearly justified, with owners clearly identified;

4.4.1.3. Providing advice, through the Chairperson, to support decisions on acceptability of risk.

4.4.2. As appropriate, Equipment/System level SECs may also be formed. Where this is the case, the interfaces between them and the relevant PSEC(s) shall be clearly defined within the respective Safety and Environmental Management Plans (SEMPs).

4.5. SQEP Panels

4.5.1. SQEP Panels shall be formed under arrangements approved by the PSEC, with members responsible for supporting Hazard Managers by ensuring that appropriate SQEP is brought to bear throughout the risk management process, particularly in identifying, reviewing and agreeing risk control measures. All SQEP panels shall include a suitably empowered representative of the relevant risk owner.

4.5.2. Whilst, for the majority of a Platform/System/Equipment life, the hazard and risk information will be reviewed by SQEP personnel who are familiar with the Platform/System/Equipment in question, there may be times when wider MOD, Industry or other stakeholders are required to review the information captured. As such, the following guidance should be considered:

4.5.2.1. Ensure that information is explained as clearly and simply as possible; although it is acknowledged that this may be difficult for some technical descriptions;

[4] Within DE&S, the eCassandra Hazard Log Tool is mandated for all projects. In 2017 the SHIPS Senior Leadership Group endorsed a phased migration of all existing Hazard Logs into eCassandra, to be completed by the end of 2020.
[5] For small BOATS, a number of classes may be covered by a single PSEC.
[6] PSECs are typically controlled and co-chaired by the relevant Platform Authority and an empowered representative of the Operating Duty Holder or other Accountable Person.

4.5.2.2. Where abbreviations or acronyms are used, ensure they are written in full at first use;

4.5.2.3. Ensure that consistent language is used. For example, refer to all working at height hazards as 'working at height' and avoid the use of 'working from height', 'fall from height', etc.

4.5.2.4. Where there is uncertainty, it is worthwhile having an independent reviewer check information prior to it being entered into the formal Hazard Log.

4.6. Hazard/Risk Communication and Escalation

4.6.1. Formal arrangements (including 'handshakes') shall be established and formally documented in SEMPs for:

4.6.1.1. The communication of Hazard/Risk related information between Equipment, System and Platform Authorities, and from Equipment/System/Platform Authorities to Duty Holders and other Accountable Persons. For risk acceptance purposes, platform primacy shall apply and risks manged by Equipment/System Authorities shall be communicated via the relevant PSEC(s).

4.6.1.2. Risk escalation, where an Authority, Duty Holder or other Accountable Person decrees that it is beyond their ability to manage or accept a Risk within the scope of their delegated or defined accountability/responsibility.

4.7. ASEMS Coherence

4.7.1. The SHIPS End-to-End Safety Risk Management Process must take due cognisance of the DE&S Acquisition Safety and Environmental Management System (ASEMS). As appropriate, existing DE&S processes are referenced (and not duplicated) within the End-to-End Process.

5. Hazard and Risk Management Planning

NOTE

- Generic requirements for Safety and Environmental Management Plans are documented in DSA01.1, DSA02-DMR, POSMS Safety Management Procedure SMP03 and the Ships OCs' S&EP O&A Statement.
- Paragraphs 5.1 to 5.7 below relate specically to the planning of Hazard and Risk Management activities.

5.1. Stage 1 of this End-to-End Risk Management Process requires that *"the SEMP shall set out the strategy for Hazard Identification and identify planned Hazard Identification activities"*, and a soundly based plan is assumed as a fundamental basis for the rest of the process.

5.2. Careful planning of Hazard Identification is a key project management discipline which is needed to lay the foundations of success for the rest of safety management activity. There is no 'one size fits all' in developing a plan of activity, and a balance needs to be struck between having a thorough and systematic approach whilst avoiding drawn-out and repetitive sessions which can become self-defeating by discouraging key SQEP from participating.

5.3. Particular planning challenges arise where equipment is being procured which is likely to be fitted to multiple ship platforms, often of different classes. Different Operating Centres may be involved, using different processes and Risk Classification Matrices. In such cases, there is clear value in the early production of a joint SEMP, covering the overall project of integrating the Equipment/System into the selected platform(s). The key to success in such a plan is the early development of a top-level safety argument to provide a convincing explanation of how the new equipment/system will be safely integrated into the ship, including all relevant support arrangements. Such an argument may typically be based upon the expected claims outlined in Box 1 below.

Safe integration has been achieved because:

- The Equipment/System being integrated has an 'inherent' level of safety (demonstrated through the Equipment/System Safety Case);
- Functional safety requirements have been identified and met.
- All dependencies and limitations identified by the Equipment/System Safety Programme/Schedule and any risks (meeting defined criteria) have been communicated to the Platform Authority and/or Duty Holder or other Accountable Person;
- All interfaces with the Platform have been identified and have been systematically risk assessed for safety by SQEP (including independent challenge);
- Identified risks have been managed to ALARP cooperatively between SHIPS Safety Authorities and other DLOD owners, with risks being accepted or escalated by the Duty Holder or other Accountable Person in line with delegated authority and recognised processes/procedures, as defined in Safety and Environmental Management Plans;
- Effective interface management and governance arrangements exist for outstanding actions and for resolution of any future identified safety issues.

Box 1: Outline Top Level Safety Argument for Equipment/System integration into Platforms

5.4. High-level claims such as those indicated above should then be used to derive the requirements for evidence and the safety activities necessary to generate such evidence. This, together with clearly defined responsibilities for their delivery, forms the core of an effective Equipment/System integration SEMP.

5.5. Early joint discussion will be needed in order to develop a coordinated strategy for suitably staged hazard identification, covering both inherent Equipment risks and those arising from installation, operation and maintenance within a Platform. In addition the functional safety role of an Equipment or System will need to be considered.

5.6. For Platform A&As, it is recommended that on initiation of CSM BP010[7], the questions in Box 2 below should be considered and answers documented and suitably reviewed, leading to a decision about whether a more comprehensive SEMP is needed.

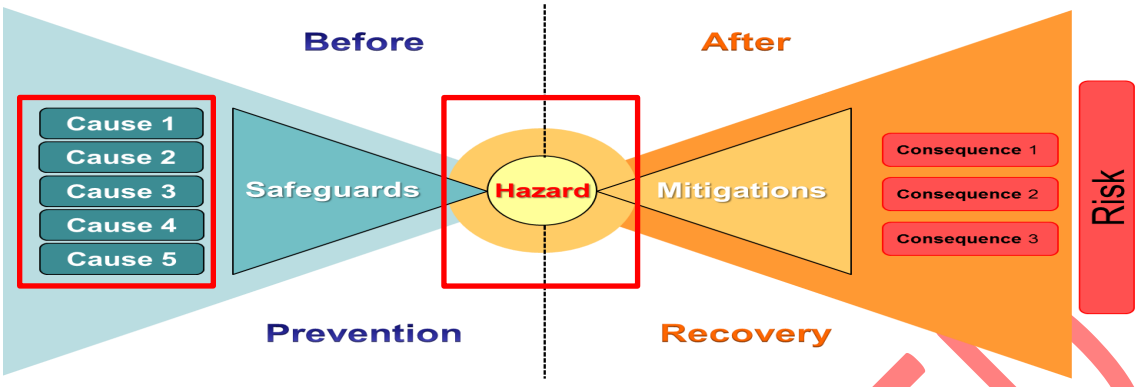
[7] Common Support Model Business Process 10 – A&A Design Change Process.

- Who is the EA lead for Safety?
- Who is the Hazard Manager for integration risks?
- What Hazard Identification activities have been (or are to be) conducted for integration risks? How are these recorded?
- What management processes exist for ensuring that integration risks are managed to ALARP? Is there/does there need to be an integrated Hazard Log?
- Does a similar process exist for managing platform safety requirements already identified by the EA?
- Have criteria/process for risk acceptance been defined and agreed by all relevant parties, and where is this documented?
- Does the need to define responsibilities and processes for effective safety integration justify a dedicated project SEMP?

Box 2: Questions to Guide the Safety Planning for Equipment/System Integration into Platforms

5.7. Once a draft SEMP has been produced, it is likely to benefit from SQEP review, and both the ISA (if appointed) and the Project Safety and Environmental Committee(s) shall be invited to provide constructive review.

6. STAGE 1 - HAZARD IDENTIFICATION



KEY RELATED DOCUMENTS

- DE&S guidance on Hazard Identification is contained within S&EP Leaflet 14/2019 and POSMS Safety Management Procedures SMP04 and SMP05.
- Some commonly used HAZID techniques are described in the ASEMS Toolkit.

6.1. Key Safety Outcomes

6.1.1. The key outcome from this stage is a thorough set of hazards, described correctly in the Hazard Log(s), which are able to be referenced back to the originating Hazard Identification activity (e.g. HAZID workshop).

6.2. Introduction

6.2.1. Hazard Identification is a through-life activity, commencing at the earliest concept of a project and continuing through into maturity in-service. During the lifecycle it is expected that the rate of identification of new hazards will diminish, but there is always potential for subtle new operating conditions or unexpected ageing mechanisms to lead to new hazards.

6.2.2. The DE&S Project Oriented Safety Management System (POSMS) identifies two stages of Hazard Identification: Preliminary Hazard Identification and Analysis (SMP04) and Hazard Identification and Analysis (SMP05). The first of these is intended to lead to an understanding of the key factors affecting the safety strategy for a project, and also to prompt early consideration of hazards which might be eliminated, preferably by design or re-design. The second stage is in reality likely to be further subdivided, with Hazard Identification activities for a warship potentially including:

6.2.2.1. Equipment/System/Platform hazards;

6.2.2.2. Equipment/System/Platform integration hazards;

6.2.2.3. Zonal-based hazards;

6.2.2.4. Activity-based hazards.

6.2.3. The SEMP shall set out the strategy for Hazard Identification and identify planned Hazard Identification activities. In this respect, it is important to remember that Hazard Identification may need to be undertaken in more than one phase, and may also benefit from both a 'top-down' approach ('risk profiling' as described in HSG65[8]) and 'bottom-up' approach (e.g. system, zone and activity based Hazard Identification). Timing is also particularly important. Conducting early Hazard Identification provides opportunities to positively influence safe design, but an immature design may not reveal all hazards. Conversely, Hazard Identification on a mature design means that design changes to improve safety may not be Reasonably Practicable and resort may be needed to procedural safeguards.

6.2.4. In addition to planned Hazard Identification, there are occasions when reactive hazard identification may be needed:

[8] Managing for Health and Safety (HSG 65) – accessible via the Health & Safety Executive (HSE) web site.

6.2.4.1. In response to modifications made to components or interfacing systems;

6.2.4.2. For urgent change of use or a new activity not previously covered by CONUSE;

6.2.4.3. In response to an accident or incident. This shall include not just the subject Platform class or Equipment/System, but any report from the international maritime community and others where there is potential for learning.

6.3. Process

6.3.1. The process diagram for Hazard Identification is shown at Figure 2 below.

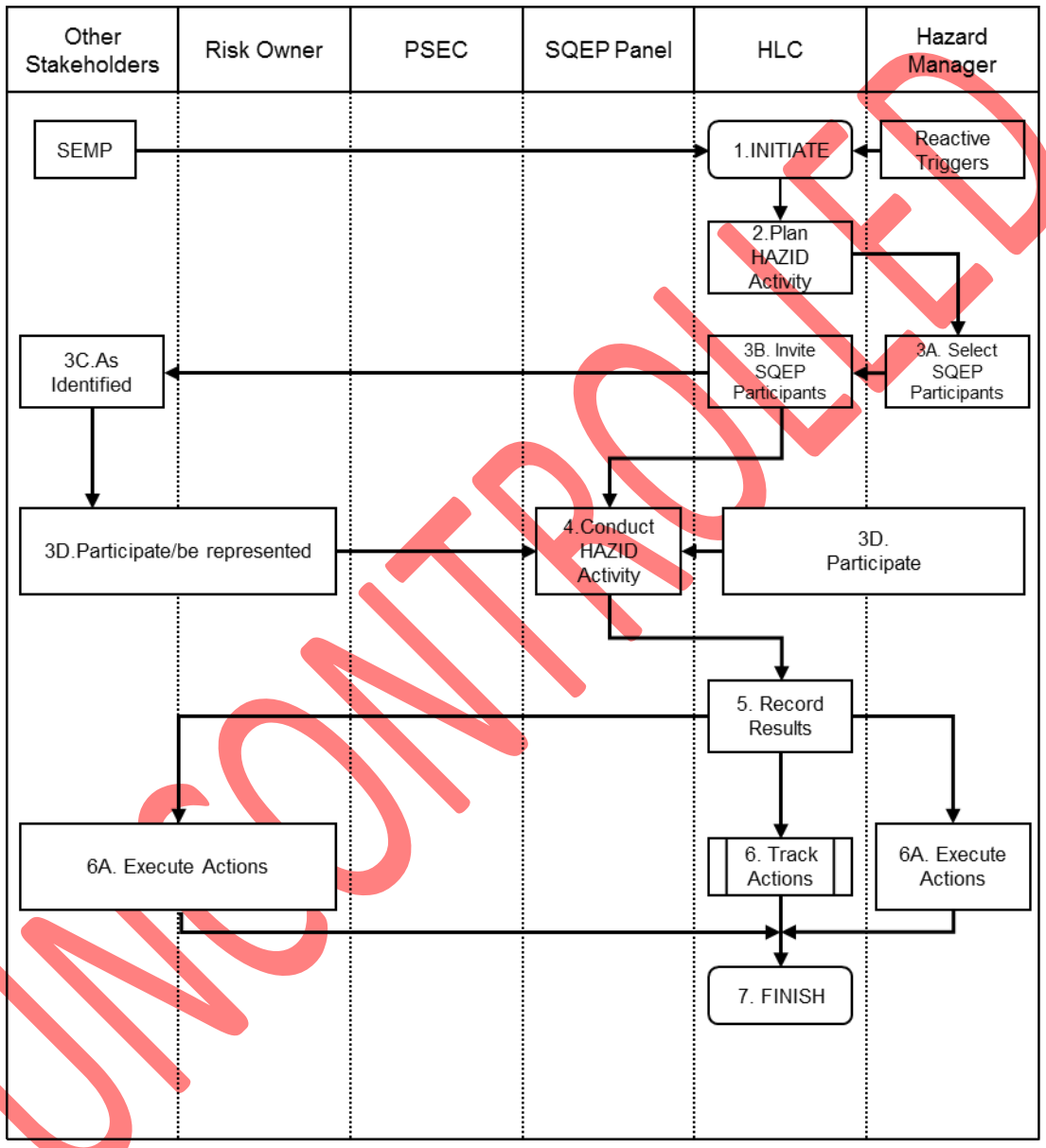


Figure 2 - Hazard Identification Process

6.4. Process Steps

6.4.1. Step 1 - Initiation

6.4.1.1. Initiation of the Hazard Identification process may be either as a planned activity derived from the SEMP, or as a reactive response to a particular trigger, for example:

1) In response to modifications;
2) For urgent change of use or a new activity not previously covered by CONUSE;
3) In response to an accident or incident.

6.4.2. Step 2 - Plan HAZID Activity

6.4.2.1. Planning of HAZID activities must be undertaken by suitably experienced safety personnel, and each HAZID session must be carefully scoped so that efficient use is made of SQEP attendees. A Briefing Pack shall be prepared for participants setting out the scope and process for the HAZID activity, and providing background briefing. There are numerous techniques available for Hazard Identification (see the Key Related Documents box above), and where multi-phase HAZID activities are intended, different techniques may be appropriate at each phase. The Briefing Pack must also include a SQEP form for all participants to complete in advance – an example template is attached at Annex A.

6.4.3. Step 3 - Select and Invite SQEP Participants

6.4.3.1. In selecting participants for a HAZID, a careful balance is needed between getting a suitably broad range of SQEP and having excessive participants; experience has shown that between seven and twelve participants is likely to give best results. Participants will depend on the subject Equipment, System, Platform or activity, but the following must be considered for inclusion as core representatives:

1) Hazard Manager (Chair);
2) Platform Authority representative;
3) Equipment/System specialist;
4) Designer/Manufacturer;
5) Naval Authority Group (NAG) representative (where applicable);
6) User representatives (both at Command and Operator/Maintainer level);
7) Other SMEs (e.g. System Design Authority);
8) SQEP facilitator.

6.4.4. Step 4 - Conduct HAZID Activity

6.4.4.1. The HAZID session must be conducted as planned. Importantly, the absence of key SQEP, particulary the User representative(s) shall require postponement, or consideration of a reduced scope and planning of an additional session.

6.4.5. Step 5 - Record Results

6.4.5.1. The primary output from the HAZID must be a set of Hazard Log entries, which are then used to trigger the Risk Analysis and Assessment process (Stage 2). Noting that HAZID activities may be undertaken without access to the Hazard Log Tool, an example template for manually capturing and recording key Hazard information is attached at Annex B. A brief record of the HAZID meeting must be made, covering:

1) Participants (name and area represented)
2) Process followed
3) Specific actions identified
4) Reference to HL entries raised

6.4.5.2. All participants must have the opportunity to review and agree the record of the meeting.

6.4.6. Step 6 - Execute and Manage Actions

6.4.6.1. Actions raised at the HAZID session must be captured, communicated to those responsible for executing them, and tracked systematically by the HLC using an appropriate tool. This is particularly important where actions are required to be completed before the next stage of the Risk Management Process (Risk Analysis and Assessment) can commence.

6.4.7. Step 7 - Finish

6.4.7.1. The HAZID process is complete when the records of the meeting have been agreed, and the Hazard Log populated to the extent possible with outputs from the HAZID meeting(s).

6.5. Guidance

6.5.1. There is much guidance on the variety of techniques that can be used in support of Hazard Identification, and the early engagement of a SQEP safety practitioner in planning effective hazard identification will be beneficial. Key points to consider are outlined in Box 3 below.

- No single technique is guaranteed to identify all hazards;
- All techniques depend on competent personnel who understand the Domain/Platform/System/Equipment in question, augmented by suitable individuals who can provide challenge to assumptions;
- Sessions need to be planned so that participants remain fully engaged. A series of short focussed sessions, with a small number of carefully selected participants may result in a more effective and efficient use of SQEP resources than full-day or multi-day events involving larger numbers. Between seven and twelve people is widely viewed as an ideal number.
- The rigour of such sessions needs to be proportionate to the likely overall risk levels;
- A structured approach is needed – this may be typically broken down by sub-system, lifecycle, activity, etc.;
- Depending on the scope, a session may undertake hazard identification and recording only, or may also include a limited amount of risk analysis and assessment.

Box 3 – HAZID Key Considerations

6.5.2. Recording Hazards

6.5.2.1. The method of recording hazards is likely to have different emphases according to the point in the Equipment/System/Platform lifecycle. Initially the main focus may purely be on Hazards, with further analysis required to capture accident sequences and assess risk scenarios. At later stages of maturity, the focus is likely to be more on Risk Control Measures and ALARP status.

6.5.2.2. It is important to ensure that the Hazards from which Risks arise are described correctly. Whilst this may seem like an obvious statement to make, experience has shown that it is not uncommon for the Hazard Description field in a Hazard Log to incorrectly describe a Hazard cause, potential accident consequence arising from the Hazard, or even a combination of these. In accordance with DEF STAN 00-056[9], a Hazard is defined as “Potential to cause harm, e.g. a physical situation or state of a system (often following from some initiating event) that may lead to an accident”. Some good examples:

1) Water on a staircase is a hazard, because there is the potential for someone to slip on it, fall and injure themselves;

2) Exposure to loud noise is a hazard because it can cause hearing loss;

3) Exposure to asbestos dust is a hazard because it can cause cancer.

6.5.2.3. Further discussion on recording Hazards/Risks is at the Hazard Log Management section of this document.

[9] Defence Standard 00-056 – Safety Management Requirements for Defence Systems.

6.5.3. Are Hazards and Risks Being Managed by the Correct Authority?

6.5.3.1. Naval Platforms are complex, and comprise a large number of systems which themselves can comprise a large number of equipments. As such, consideration needs to be given to the following:

1) The intrinsic risks posed by Equipment, e.g. Gearbox explosion;

2) The safety impact of the functions an Equipment performs, e.g. Gearbox failure leading to loss of propulsion;

3) The Risks that may arise from integrating the Equipment into a higher-level system, e.g. misalignment of shaft between Engine and Gearbox;

4) Operating Risks, e.g. working in confined spaces.

6.5.3.2. It is therefore important that Hazards and Risks are managed[10] by the appropriate Authority:

6.5.3.3. The intrinsic risks of an Equipment are generally managed by the Equipment Authority.

6.5.3.4. Risks arising from the functional failure of Equipment or its integration into a wider System should be managed at the system level, by either the System or Platform Authority. NOTE: It is recognised that, in some areas, Equipments Teams provide Equipment direct to the User as opposed to it being integrated into a System/Platform (e.g. Sea Survival Equipment, Trainers, etc.). In such cases, it will be appropriate for functional related Risks to be managed by the Equipment Authority.

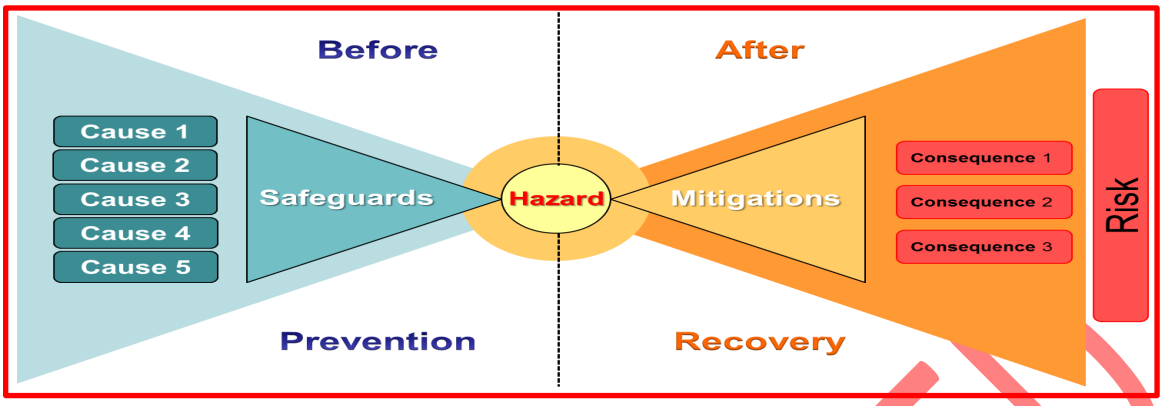
6.5.3.5. Operating Risks will be likely be managed by the Operating/Delivery Duty Holder or other Accountable Person.

6.5.3.6. Where there is doubt about whether a Hazard/Risk should be managed at Platform, System or Equipment level, the principle of Platform Primacy must apply and the PA must take the lead until a clear case can be made for transferring Hazard/Risk management.

6.5.3.7. ☞☜ A 'handshake' process to facilitate Hazard communication between Authorities and Duty Holders or other Accountable Persons is attached at Annex C. This process is to be used where it is identified that Hazards/Risks are being managed by the incorrect Authority (e.g. equipment functional failures that do not present an immediate risk of harm being incorrectly managed within Equipment Authority Hazard Logs).

[10] Whilst the overall management of a Risk lies with the nominated Hazard Manager, it is important to recognise that the various individual Risk Control Measures for a particular Risk will likely be owned by different Authorities (EA, PA, DDH, etc.)

7. STAGE 2 - RISK ANALYSIS AND ASSESSMENT



KEY RELATED DOCUMENTS

- DE&S guidance on Risk Estimation is contained within S&EP Leaflet 14/2019 and POSMS Safety Management Procedure SMP06.
- Some commonly used tools to assist with risk analysis and assessment are described in the ASEMS Toolkit.

7.1. Key Safety Outcomes

7.1.1. The outcome from this stage is understood and correctly classified risks are recorded in the Hazard Log, providing the basis for subsequent prioritised management action.

7.2. Introduction

7.2.1. As per DE&S policy, the recognised means for assessing levels of safety risk is the risk matrix, which combines values of severity and likelihood to categorise risk in the range A to D, where Class A risks are the highest. The process is primarily intended to aid judgement by ranking risks; the individual risk classifications should not be seen as representing a precise measure of risk.

7.2.2. The Ships OCs' Risk Classification Matrix at Annex D provides the basis for assessment of all risks within this process. Analysis of accident sequences arising from an identified Hazard need to consider both credible worst case and most likely outcomes. The probabilities of each need to be assessed and an overall risk classification selected.

7.2.3. Risk assessment must be undertaken in the knowledge or assumption of existing controls. Assumptions must be recorded and subsequently validated prior to declaration of 'ALARP' and as part of on-going risk review. Governance activities are determined by the highest level of risk.

7.2.4. Risk analysis and assessment undertaken by Equipment Authorities may not have full knowledge of actual or potential additional risk controls at System and/or Platform level, or those implemented by the Operator. Therefore, the inclusion of suitably experienced System/Platform Authority and Duty Holder/Accountable Person representatives within Equipment SQEP Panel meetings is important to provide such knowledge, but where this is not possible risk assessments must be both provisional and pessimistic, and must prompt a reassessment of risk when the full operational context for use is understood.

7.3. Process

7.3.1. The process diagram for Risk Analysis and Assessment is shown at Figure 3 below.

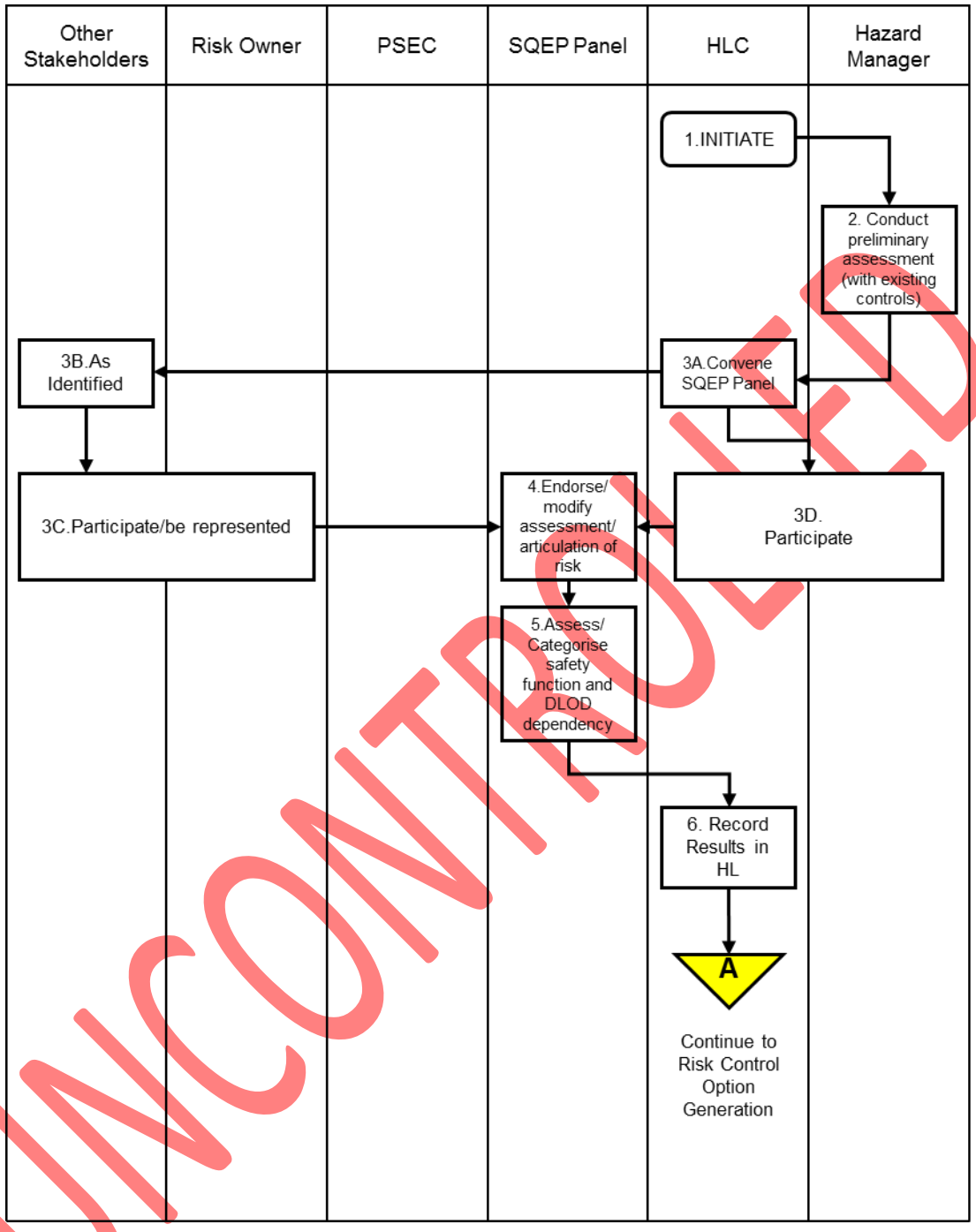


Figure 3 – Risk Analysis and Assessment Process

7.4. Process Steps

7.4.1. Step 1 - Initiation

7.4.1.1. The activity is initiated by the HLC on behalf of the Hazard Manager, and may cover one or more Hazards identified by the previous stage.

7.4.2. Step 2 - Preliminary Assessment

7.4.2.1. The Hazard Manager shall make a preliminary assessment of the Risks arising from the Hazard(s), according to the Ships OCs' Risk Classification Matrix at Annex D. Such assessment shall include both the most likely outcome and the credible worst case. The provisional classification must reflect the more pessimistic result, and assessment must be based upon known existing controls before the application of any additional risk control measures.

7.4.3. Step 3 - Convene SQEP Panel

7.4.3.1. The HLC must convene a SQEP panel with sufficient expertise to fully understand the Risks arising from the Hazards under consideration. As a minimum, the following must be included or represented:

1) Hazard Manager (Chair)
2) Empowered representative of the Risk Owner;
3) Platform Authority;
4) Equipment/System Authority;
5) User representative;
6) Other SMEs as appropriate;

7.4.3.2. All SQEP Panel participants must complete a SQEP form in advance – an example template is attached at Annex A;

7.4.3.3. For urgent consideration of emergent hazards on in-service systems, the formation of a SQEP panel may be by any suitable means including VTC, conference call, or e-mail exchange, subject to appropriate recording (see section on Hazard Log Management).

7.4.4. Step 4 - Endorse/Modify Assessment of Risk

7.4.4.1. The SQEP Panel must review the provisional classification assigned by the Hazard Manager and make any necessary adjustments.

7.4.5. Step 5 - Assess/Categorise Safety Function and DLOD Dependency

7.4.5.1. The SQEP Panel shall assess:

1) Any Platform Safety Functions which are affected by the risk under assessment. Guidance on the SHIPS Safety Function Model is at Annex H;
2) The level of dependency (High/ Medium/ Low) on other (i.e. non Equipment) DLODs. For HIGH, this shall further identify whether particular Training, Procedure, or Logistics requirements exist to enable effective risk control.

7.4.5.2. The intent behind each of these categories is to enable more effective cumulative risk identification and control at both PA and Duty Holder or Accountable Person levels. The categories are expected to act as triggers for review at these levels of the cumulative effects of all risks so identified.

7.4.6. Step 6 - Record Results in HL

7.4.6.1. The results of this activity shall be recorded in the Hazard Log by the HLC. A brief record of the SQEP Panel meeting including attendance, issues discussed and decisions/actions must be maintained within Project Safety Records.

7.4.7. A - Continue to Risk Option Generation

7.5. Guidance

7.5.1. Risk Analysis and Assessment considers the range of possible ways in which a Hazard might lead to harm to people and classifies the risk according to the combination of consequence and probability of occurrence. For SHIPS Safety Authorities, the SHIPS Risk Classification Matrix at Annex D is mandated. Where different RCMs are involved, either as a result of incorporation of legacy safety work, or where other Operating Centres are involved, then the means of reconciling these different systems needs to be agreed and documented early in a combined SEMP (see section on Hazard and Risk Management Planning).

7.5.2. For each hazard identified, the potential Accident Severity, Frequency of Harm and resulting Risk Classification shall be assigned in accordance with the Ships OC Risk Classification Matrix at Annex D. In the case of non-fatal accidents, the matrix includes definitions of the types of injuries and illnesses that fall into the Major, Marginal and Negligible categories.

7.5.3. Accident Severity Assessment

7.5.3.1. MOD policy requires that all credible outcomes associated with a Hazard are identified and managed. As a minimum, the risk analysis and assessment shall ensure the worst credible outcome has been considered. Where it can be demonstrated that the accident sequences and associated control measures (and hence accident probability) are the same for all credible outcomes, it is acceptable to take a proportionate approach by recording and managing Risk associated with the worst credible outcome (and hence highest Risk level) only. For example, consider the hazard of an exposed electrical conductor during live working - electrocution (death) and recoverable injury from electric shock are both credible outcomes associated with contacting with the live conductor, electrocution being the worst credible. Before control measures are applied, electrocution will have a higher Risk Classification. Any control measures that reduce the probability of electrocution (insulated tools, PPE, procedures, training, etc.) will also reduce the probability of electric shock; hence risk governance shall be in accordance with the electrocution risk.

7.5.3.2. Where different outcomes associated with the same Hazard have different accident sequences and control measures, it is possible that the increased probability of a lower level of harm will result in a higher level of Risk. For example, consider someone falling overboard from a Ship - drowning and recoverable injury (such as hypothermia) are both credible outcomes, with drowning being the worst credible. Before mitigations are applied, drowning will have a higher Risk Classification. A control measure that reduces the likelihood of drowning (e.g. lifejacket) will provide little or no protection against the effects of the cold and hence will not reduce the likelihood of hypothermia. It is therefore possible that the Residual Risk associated with hypothermia may be higher than for drowning. In such instances, both Risks must be recorded in the Hazard Log and managed according to their Risk Classification.

7.5.4. Frequency Assessment

7.5.4.1. Whereas it is possible to predict the consequences of an accident with a relatively high degree of confidence, frequency of harm is far more subjective and hence more difficult to assess. In conducting the risk analysis and assessment, a judgement must be made on whether the predicted frequency of harm is realistic, based on the data/analysis available and the number/robustness of control measures in place. This judgement must take account of:

1) Assessed frequency of initiating events;
2) Likelihood of initiating events resulting in the Hazard occurring, taking into account the preventative control measures (Safeguards) in place;
3) Likelihood of the hazard leading to the identified accident, taking into account the reactive control measures (Mitigations) in place.

7.5.4.2. For example, if a particular Hazard has multiple potential causes and identified control measures are limited to a small number of drills/procedures, it is reasonable to expect that the predicted frequency of harm would be relatively high. On the other hand, if there is a wide range of robust control measures, including

engineered solutions, then the predicted frequency of harm should be relatively low. Information available to support this judgement may include:

1) Quantitative analyses such as Fault Trees and Event Trees;
2) Past experience/precedent. Note: whilst it is useful to note that the modern Navy has around 10,000 ship years of peacetime operating experience, caution must be exercised in over reliance on past precedent, especially where there is no evidence to substatinate assertions;
3) Professional judgement of SQEP;
4) Accident and incident data.

7.5.4.3. Risk estimation must always err on the side of safety, recognising in particular that it can be difficult to accurately estimate the frequency of low likelihood events. The Precautionary Principle[11] must be applied for any areas of uncertainty – for ease of reference, the relevant guidance from the Defence Maritime Regulator (DMR) is reproduced in Box 4 below.

The Precautionary Principle

The precautionary principle describes the philosophy that must be adopted for addressing Risks subject to high uncertainty, and rules out lack of certainty as a reason for not taking preventative action. The precautionary principle must be invoked where:

- There is good reason, based on empirical evidence or plausible causal hypothesis, to believe that serious harm might occur, even if the likelihood of harm is remote;

  and;

- The information gathered reveals such uncertainty that it is impossible to evaluate the outcomes with sufficient confidence to move to the next stage of the risk assessment process.

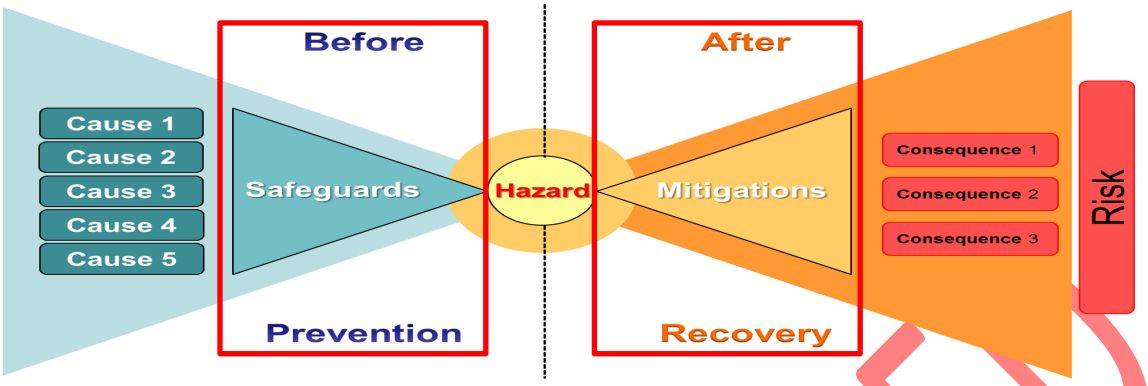
Box 4 – The Precautionary Principle

7.5.5. Risk Classification

7.5.5.1. Having confirmed that the Accident Severity and Frequency of Harm are correct, the Risk Classification shall be checked to ensure that it is reflects the assigned levels; this is particularly important where the SQEP Panel risk analysis and assessment has necessitated changes to the Hazard Manager's preliminary assessment. Where this results in a change to the Risk Classification, the Risk will need to be managed accordingly. For example, a Risk that is re-classified from a D to a C will subsequently require a more robust ALARP justification/statement.

[11] As described in the HSE *Reducing Risks, Protecting People* document.

8. STAGE 3 - GENERATING OPTIONS FOR RISK CONTROL



KEY RELATED DOCUMENTS

- DE&S Policy on demonstrating ALARP in a Military Equipment Capability Context is contained within DE&S S&EP Leaflet 02/2011.
- DE&S guidance on Risk and ALARP Evaluation is contained within S&EP Leaflet 14/2019 and POSMS Safety Management Procedure SMP07.
- DE&S guidance on Risk Reduction is contained within S&EP Leaflet 14/2019 and POSMS Safety Management Procedure SMP08.

8.1. Key Safety Outcomes

8.1.1. The outcome of this stage is the identification of a range of possible risk reduction options for subsequent consideration and agreement by the SQEP Panel, against ALARP criteria.

8.2. Introduction

8.2.1. This activity will often be undertaken concurrently with Risk Analysis and Assessment (Stage 2) and/or decisions making on implementing Risk Control Measures (Stage 4). However, although a simple stage in principle, it is included as a separate activity here in view of its importance in ensuring that the full range of options are considered. This enables strong ALARP arguments to be made, based both upon options taken forward for implementation and those that are not (with supporting justification).

8.2.2. For Hazards identified during the design phase, the generation of options for risk control can reasonably be undertaken as a discrete activity and sequentially within the overall process. However, for in-service hazards the consideration of possible risk controls must be started as soon as a Hazard is identified. In particular, operating constraints may be appropriate until a better understanding of the precise nature of a Hazard is understood and the reasonable practicability of potential Risk Control Measures established.

8.3. Process

8.3.1. The process diagram for Generating Options for Risk Control is shown at Figure 4 below.

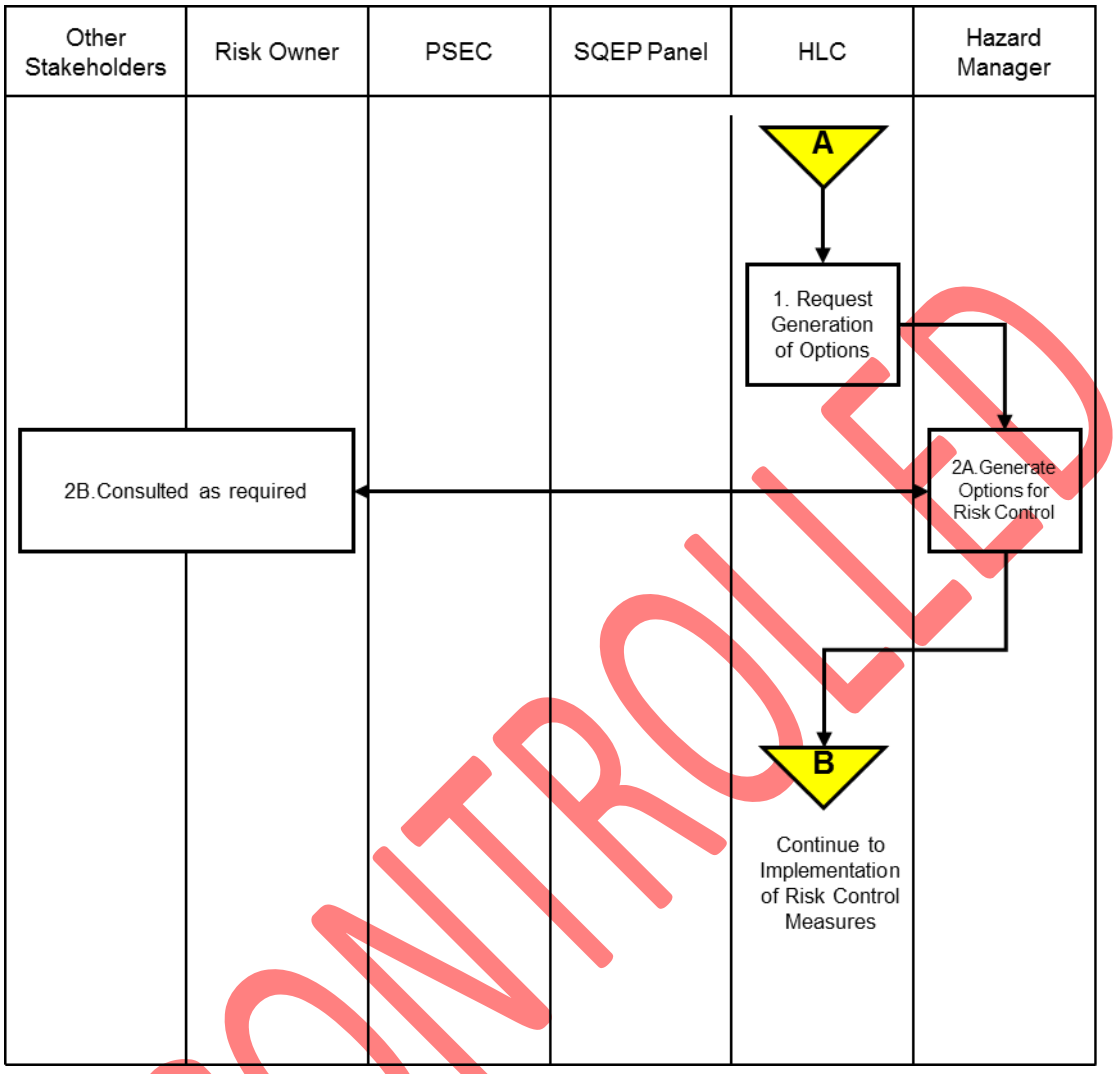


Figure 4 – Generating Options for Risk Control Process

8.4. Process Steps

8.4.1.A - Initiation

8.4.1.1. This stage follows on from Risk Analysis and Assessment

8.4.2.Step 1 - Request Generation of Options

8.4.2.1. The stage is prompted by the HLC who must request the Hazard Manager or technical lead to consider potential Risk Control Measures in advance of a formal SQEP Panel meeting.

8.4.3.Step 2 - Generate Options

8.4.3.1. The previous activity within this the End-to-End Risk Management Process will have resulted in Risks being classified based on known existing controls. The Hazard Manager must now consider whether further Risk Control Measures must be implemented to demonstrate ALARP. In certain circumstances (e.g. an emergent in-service issue), the Hazard Manager may recommend the immediate implementation of temporary measures such as ceasing/limiting the operation of an Equipment/System.

8.4.3.2. The following set of questions must be considered (ideally in advance of a SQEP Panel being convened) by the Hazard Manager:

1) Is there a current risk to life, or uncertainty as to level of safety, which might justify operating restrictions or, in extreme circumstances, the withdrawal of an Equipment/System from service? If so, have these been discussed with appropriate representattives of the Duty Holder or Accountable Person?

2) Is the Hazard adequately understood, and if not, what options are possible for improving understanding?

3) Has Design Authority/OEM advice been sought/obtained (where relevant)?

4) What is the physical location? Does this introduce additional factors?

5) What technical options exist for removing or controlling the Hazard? What potential timescale/cost is involved with each of these?

6) Are there any specific legislative/regulatory requirements?

7) What constitutes recognised good practice?

8) Are any interim engineered safeguards possible pending a long term solution?

9) What procedural controls can be introduced? Are these needed on a permanent or a temporary basis?

10) Is there scope for risk controls to be implemented concurrently (e.g. by EA/PA/ODH)?

11) Do introduced risk controls have potential to generate new Hazards, and is a formal hazard identification activity needed?

12) What documentation/training is needed to support various risk control options?

8.4.3.3. As prompted by the questions above, the Hazard Manager may need to consult with other stakeholders in developing a suitable range of options. Such stakeholders may include (but not be limited to):

1) Duty Holder or Accountable Person representative;

2) PA/EA/System DA representatives;

3) Other PAs (e.g. to consider recognised good practice);

4) Manufacturer/Industry specialist.

8.4.3.4. Options must be documented proportionately to risk and in a way that supports SQEP panel discussion and eventual generation of an ALARP Statement.

8.4.4.B - Continue to Implementation of Risk Control Measures.

8.5. Guidance

8.5.1. In essence, demonstrating ALARP requires that the following conditions are met:

8.5.1.1. Compliance with Legislation/Regulations;

8.5.1.2. Compliance with good practice;

8.5.1.3. Demonstration of Reasonably Practicable.

8.5.2. Satisfying Relevant Legislative/Regulatory Requirements

8.5.2.1. Duty Holders and other Accountable Persons[12] are responsible for identifying the Legislative and Regulatory requirements applicable to their Equipments/Systems/Platforms. In accordance with the SofS Policy Statement[13], where there are exemptions or derogations from legislation applicable to Defence, standards and arrangements shall produce outcomes that are, so far as reasonably practicable, at least as good as those required by legislation.

[12] In the context of this section, it must be recognised that the responsibilities placed on Duty Holders may be discharged by others who have been formally authorised to act on their behalf.

[13] DSA 01.1 Chapter 1 - The Secretary of State's Policy Statement for Health, Safety and Environmental Protection in Defence.

8.5.3. Absolute Requirements

8.5.3.1. The words ‘shall’ or ‘shall not’, used in statutory provisions, impose an absolute obligation to do, or not do, the act in question.

8.5.4. Practicable Obligations

8.5.4.1. Where an obligation is qualified by the word ‘practicable’, the standard is stricter than ‘reasonably practicable’ and Duty Holders or Accountable Persons must do what is necessary to reduce the risk regardless of the cost (in time or money), provided that the measures are possible in the light of current knowledge and invention, e.g. the requirement to fit guards on rotating machinery.

8.5.5. Complying with Good Practice

8.5.5.1. The HSE is clear that, where there is relevant, recognised good practice, Duty Holders or Accountable Persons are expected to follow it. Where Duty Holders or Accountable Persons are unable to apply good practice or choose to do something different, they must be able to demonstrate that the measures they propose to use are at least as effective in controlling the Risk.

8.5.5.2. Good practice refers to measures, actions, procedures or specifications considered appropriate by professionals based on either experience of their application or a consensus view. Often, demonstrating that good practice has been applied will remove the need to assess safety risks from first principles. However, this cannot be assumed and each Risk will need to be considered on a case-by-case basis.

8.5.5.3. Good practice in the Maritime domain can include (but is not limited to):

1) HSE/MCA/IMO Codes of Practice and Guidance Notes;
2) Classification Society Rules;
3) British and EN standards;
4) Defence or NATO Standards;
5) OEM Company Standards.

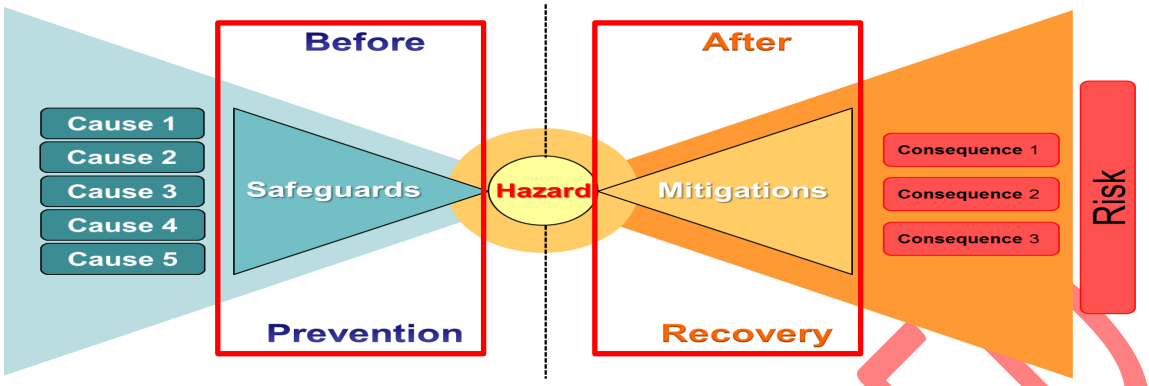
8.5.5.4. It is important to recognise that good practice evolves, i.e. what is considered good practice today may not be so tomorrow. Therefore, it is essential that those conducting the review are able to satisfy themselves that, where appropriate, Risk Control Measures reflect current good practice, particularly where a Risk may not have been reviewed for some time. Furthermore, where planned future changes to good practice are known, the Hazard Log/Action Plan must include appropriate actions to review at the relevant time.

8.5.6. Demonstrating Reasonably Practicable

8.5.6.1. As a minimum, Hazard Managers must ensure that Legislative/Regulatory requirements have been met and recognised Good Practice applied. In many instances, this may be sufficient to achieve ALARP, especially if the Residual Risk is deemed to be Broadly Acceptable. However, this cannot be assumed and each Risk must be considered on a case-by-case basis.

8.5.6.2. If the application of good practice is not deemed sufficient to demonstrate ALARP, (or if there is no relevant good practice) the Hazard Manager will need to examine what other options exist to reduce the Risk. Ultimately, the onus is on Duty Holders or Accountable Persons to demonstrate that they have considered all reasonably foreseeable options, and this will require an appropriate level of SQEP in both safety management and the Equipment/System/Platform/Activity under consideration. This analysis must follow the recognised mitigation hierarchy, as defined in POSMS SMP08.

9. STAGE 4 - IMPLEMENTING RISK CONTROL MEASURES



KEY RELATED DOCUMENTS

- DE&S Policy on demonstrating ALARP in a Military Equipment Capability Context is contained within DE&S S&EP Leaflet 02/2011.
- DE&S guidance on Risk and ALARP Evaluation is contained within S&EP Leaflet 14/2019 and POSMS Safety Management Procedure SMP07.
- DE&S guidance on Risk Reduction is contained within S&EP Leaflet 14/2019 and POSMS Safety Management Procedure SMP08.

9.1. Key Safety Outcomes

9.1.1. The outcome of this stage is a set of defined actions and risk control measures which are recorded and monitored through to completion, in order to support an ALARP justification.

9.2. Introduction

9.2.1. This activity is about deciding which Risk Control Measures from the options generated during Stage 3 must be implemented to demonstrate ALARP. The working assumption underpinning this stage is that suitably empowered and competent personnel, including importantly Duty Holder or Accountable Person representatives, are brought together to review and decide risk control actions in the context of expected operational needs. This enables a number of actions to be undertaken in parallel in order to drive risk to ALARP at the earliest point. When risks are being sentenced as part of a design process for an Equipment/System/Platform not yet in-service, the immediate requirement for risks to be ALARP does not apply and a sequential approach to actions may be appropriate.

9.2.2. The Hazard Manager shall lead the decision making process about which risk control measures are to be implemented. In doing this, he/she must ensure that he/she is suitably supported by SQEP from other technical organisations as well as with suitable Duty Holder or Accountable Person representation and suitable Safety Management SME. In general, it is appropriate for the EA to act as Hazard Manager where all or most of the likely risk controls are within his/her ability to implement, or where the Equipment is fitted to different classes of platform. Where hazards originating from an Equipment/System require wider control measures including coordinated actions by PA and Duty Holder or Accounatble Person, and particularly where a single class of platform is involved, it is likely that effective risk management may best be coordinated by the PA.

9.2.3. The SQEP Panel will normally form the decision making group, both with regard to the reasonable practicability of risk reduction measures, and to the credibility of an ALARP statement. Such a group is likely to meet at regular intervals according to Project need, but SEMPs shall provide for 'virtual' meetings (e.g. by email exchange or via VTC) in order to address urgent emerging issues. In smaller projects, the SQEP Panel role may be undertaken by the PSEC. In large projects, it is likely that a number of SQEP Panels will be required to provide advice and assurance to the PSEC, likely aligned to the related high level hazards.

9.2.4. Regardless of where the accountability lies for completing actions and/or implementing Risk Control Measures (EA, PA, DDH, etc.), all such activities shall be monitored through to completion by the nominated Hazard Manager, and evidence of such completion is required before the status of such risks can be changed from OPEN or MANAGED to ALARP. If the Hazard Manager resides in DE&S, it is particularly important to ensure that actions placed on Navy Command (relating to other DLODs) are formally communicated and acknowledged by the appropriate owner, and that the Hazard Manager undertakes 'closed loop' monitoring on behalf of the Risk Owner.

9.3. Process

9.3.1. The process diagram for Implementing Risk Control Measures is shown at Figure 5 below.

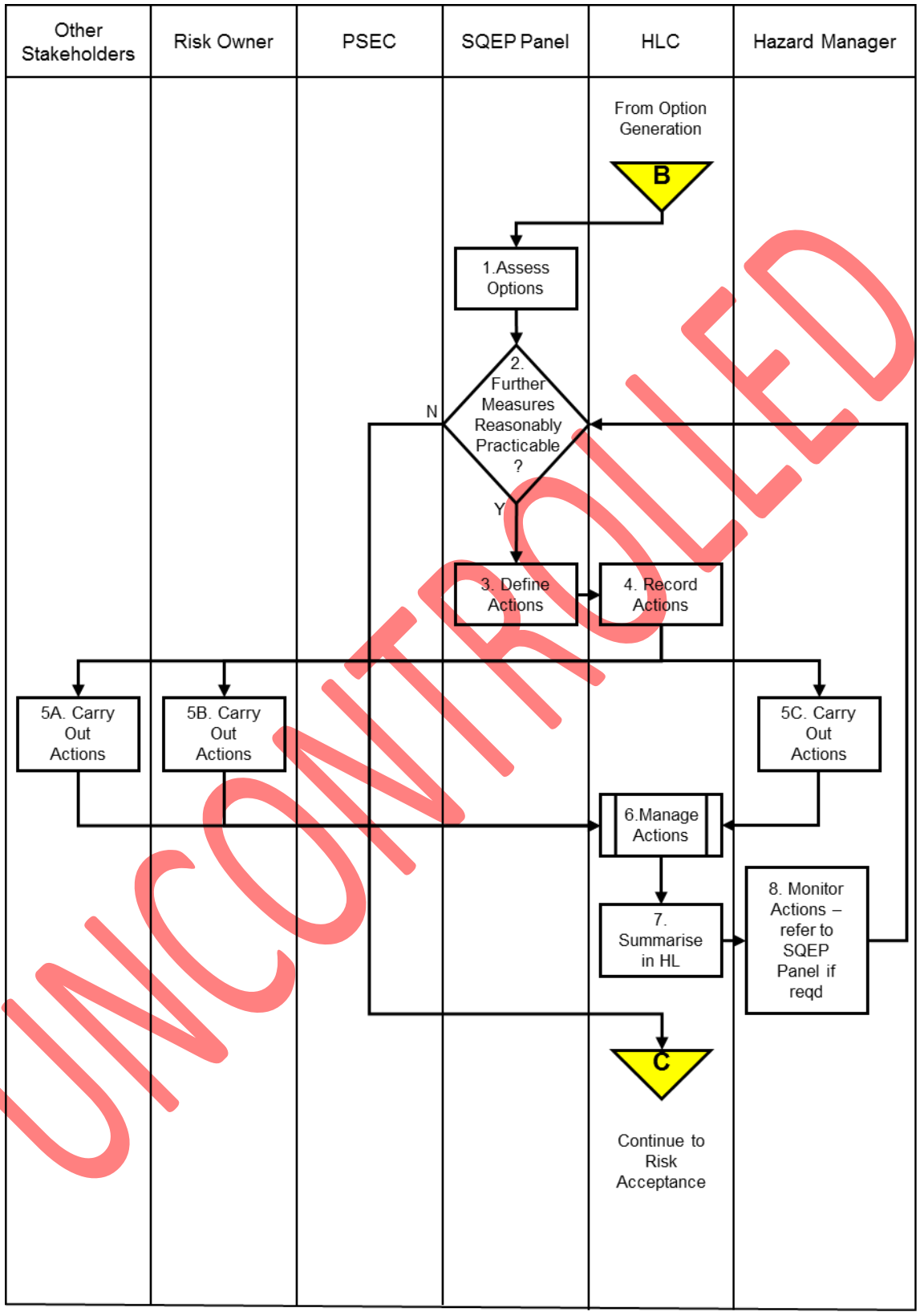


Figure 5 – Implementing Risk Control Measures Process

9.4. Process Steps

9.4.1. B - Initiation

9.4.1.1. This stage follows on from Option Generation.

9.4.2. Step 1 - Assess Options

9.4.2.1. This is undertaken by a suitably convened SQEP panel, and the discussion must consider the options generated under Stage 3. The following factors must be considered:

1) Feasibility of options
2) Combinations/sequences of options
3) Implementation opportunities
4) Effectiveness of risk reduction/control
5) Counter-risks from changes
6) Costs (time, effort, operational capability)

9.4.3. Step 2 - Decision on whether further measures are Reasonably Practicable

9.4.3.1. The panel shall decide which measures are reasonably practicable in accordance with the ALARP principle (and HSE and MoD guidance) in a way that can be suitably justified in an ALARP statement. During this activity, the Hazard Manager must develop a draft ALARP statement which shall inform the SQEP panel deliberations and be updated to reflect agreed actions. Guidance on the proportionality of ALARP Statements is contained at Annex G.

9.4.4. Step 3 - Define Actions

9.4.4.1. Actions may include both investigative tasks and actual implementation of Risk Control Measures. The SQEP Panel chair shall ensure that actions are defined in terms of the outcomes to be achieved, action owner, and date for achievement. The prioritisation of actions must be proportionate to risk.

9.4.5. Step 4 - Record Actions

9.4.5.1. The HLC shall record agreed actions. The Hazard Manager is accountable for ensuring that actions are formally communicated to, and formally acknowledged by, the relevant owner.

9.4.6. Step 5 - Carry Out Actions

9.4.6.1. Once actions have been formally communicated and acknowledged, the relevant action owners are accountable to the Hazard Manager for their completion in accordance with agreed timescales and for the formal confirmation of such.

9.4.7. Step 6 - Manage Actions

9.4.7.1. The HLC shall ensure that actions are managed systematically and are not closed off until adequate evidence of completion is provided, to the satisfaction and agreement of the Hazard Manager.

9.4.8. Step 7 - Summarise in HL

9.4.8.1. The HLC shall ensure that the HL is kept updated with a summary of the status of risk control actions.

9.4.9. Step 8 - Monitor Actions

9.4.9.1. The Hazard Manager, supported by the HLC, shall monitor the progress and completion of actions, and the effectiveness of the measures taken in order to ensure that an ALARP position is maintained throughout. The SQEP panel shall be consulted and/or reconvened as required to consider any failures to meet the intent of actions, and concerns shall be escalated as appropriate to the Risk Owner.

9.4.10. C - Continue to Risk Acceptance.

9.5. Guidance

9.5.1. Once potential Risk Control Measures are identified, the SQEP panel must establish whether it is reasonably practicable to apply them. This will require appropriate SQEP to consider:

9.5.1.1. Practicable. Technology and/or processes exists and could be applied;

9.5.1.2. Reasonable. Sacrifice (money, time and effort) is not Grossly Disproportionate to the benefit.

9.5.2. If the decision is taken to implement an additional Risk Control Measure, consideration must be taken of its potential effect on other Risks associated with the Equipment/System/Platform. In some cases, a new Risk Control Measure may provide additional mitigation across a number of risks (e.g. training to improve operator SQEP). However, it is also important to recognise that mitigating one risk might have a negative impact on another. For example, increasing the frequency of machinery space inspection rounds to reduce the probability of a fire going undetected might increase the operator's exposure to other risks such as arc flash. Similarly, increasing the frequency of maintenance to reduce the risk of a safety critical system failure may increase operator exposure to intrinsic risks (e.g. electric shock, hydraulic fluid release, arc flash, etc.) and may also increase the risk of a maintenance related error.

9.5.3. Gross Disproportion

9.5.3.1. Risk Control Measures deemed practicable to implement can only be discounted on the grounds of gross disproportionality. As highlighted in DE&S S&EP Leaflet 02/11, the concept of Gross Disproportion requires Duty Holders or Accountable Persons to weigh the sacrifice (money, time and effort) involved in a risk reduction option against its risk reduction benefits. Specifically, a risk reduction option must be implemented if the sacrifice (or cost) is not grossly disproportionate to the benefit achieved. Insufficient funding alone is not a justification for not implementing a practicable risk reduction option.

9.5.3.2. Often, it will be possible to reach a gross disproportion decision through simple qualitative analysis, i.e. by applying common sense and/or exercising professional judgement or experience. Using some extreme examples:

1) Spending £1M to prevent someone suffering a bruised knee once a year is obviously grossly disproportionate;

2) but;

3) Spending £1M to prevent a major explosion capable of killing 150 people in a single event is obviously not grossly disproportionate.

9.5.3.3. Where the situation is less clear cut, it may be necessary to undertake a more detailed comparison using formal Cost Benefit Analysis (CBA), which aids the decision making process by giving monetary values to the costs and benefits to enable a comparison of like quantities. There is no authoritative guidance on when CBA should be applied; however, HSE guidance indicates that it might typically be required when:

1) Established good practice does not exist or is out of date;

2) The situation is complex and the relevance of individual good practice is questionable e.g. the combination of discrete hazards is not foreseen in good practice documents;

3) "High Hazard" scenarios.

9.5.3.4. Further guidance on Cost Benefit Analysis, including worked examples, is contained in at Annex E and in a number of HSE documents (references A to D).

9.5.4. Assuring Risk Control Measure Implementation

9.5.4.1. Before a Control Measure can be considered to provide risk mitigation, it must be confirmed that it is current and has been implemented. Recognising that individual Risk Control Measures for a particular Risk may be owned by different Authorities, it is important to ensure that this stage of the process involves/consults with appropriate representatives from all relevant stakeholders to confirm control measure implementation. To enable this to happen, it is important to ensure that

Risk Control Measures are described in sufficient detail to provide a clear audit trail. As a minimum, Risk Control Measure information shall include:

1) A reference for the mitigation, e.g. BR reference for a procedure, relevant Defence Standard, report reference for a survey report, etc.;

2) Currency of the control measure, e.g. date of publication and review/expiry date if known. This is particularly pertinent where measure are introduced via a temporary means (RNTM, S2022A, etc.);

3) A Risk Control Measure Owner.

9.5.4.2. Commonly identified shortfalls in identifying Risk Control Measures include phrases such as:

1) “Training” – but no reference to specific courses.

2) “Procedural Control” – but no reference to specific documents, e.g. BRs or SOPs.

3) “Design Feature” – but no reference to specific design standards.

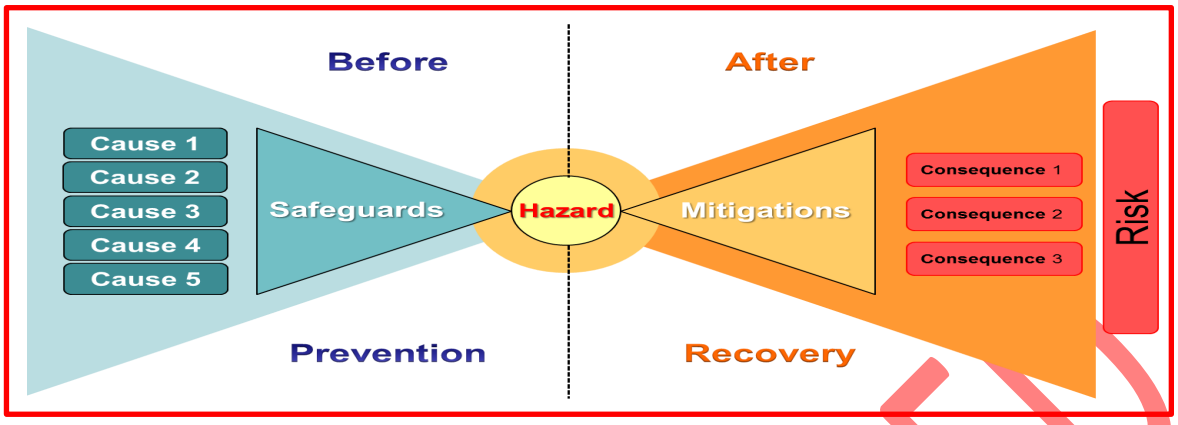
4) “To be”/”will be” – care must be taken not to confuse existing mitigations with actions which beed to be completed in order to provide a mitigation.

9.5.4.3. **Note:** In May 2014, in support of the Ships OC Safety Risk Review Programme, the Ships OCs' S&EP Team Leader issued guidance to clarify the position regarding ownership of Risk Control Measures by Ships OC Safety Authorities and other DLOD owners; key extracts from this note are reproduced at Annex F, with terminology updated to reflect subsequent changes/developments.

9.5.5. Overdue Actions

9.5.5.1. It is important to recognise that not all overdue actions related to the implementation of Risk Control Measures will necessarily compromise the ALARP status of a Risk. For example, an Equipment maintainer may be working to revised instructions contained within a Temporary Engineering Bulletin (TEB), pending formal update of a BR. If the BR update is delayed beyond the action target date, then provided that the TEB remains current and available to the maintainer, the ALARP status of the associated Risk will not be compromised.

10. STAGE 5 - RISK ACCEPTANCE



KEY RELATED DOCUMENTS

- DE&S policy on Equipment Safety and Environmental Protection (SEP) Risk Referral is contained within DE&S S&EP Leaflet 03/2011.
- DE&S guidance on Risk Acceptance is contained within POSMS Safety Management Procedure SMP09.

10.1. Key Safety Outcomes

10.1.1. The outcome of this stage is ALARP risks that are recorded as having been accepted by, or on behalf of, the relevant Duty Holder or Accountable Person. Alternatively, a risk may not be accepted, and reconsideration of risk controls prompted.

10.2. Introduction

10.2.1. All risk acceptance is undertaken by or on behalf of the Duty Holder or Accountable Person, and such arrangements must be clearly documented in SEMPs. Whilst Ships OCs' Safety Authorities might make recommendations to a Duty Holder or Accountable Person on the ALARP status of risks, they are not permitted to accept such risks. Where appropriate, SEMPs may describe sub-delegations from Safety Authorities to defined assignment holders for making ALARP recommendations - see Leaflet 14 of the SHIPS OCs' S&EP O&A Statement.

10.2.2. Risk acceptance includes both a SQEP judgement that all reasonably practicable risk reduction measures have been implemented (ALARP), or are planned (MANAGED), and also a decision about Tolerability. The normal threshold for 'UNACCEPTABLE' risk is set at the Class A/B boundary, but MOD guidance recognises that situations arise where Class A risks may need to be accepted for operational reasons and also where lower classification risks may be regarded as not able to be tolerated where there is not a compelling operational need and/or further risk reduction is achievable. DE&S S&EP Leaflet 03/2011 defines a process for risk referral, i.e. for situations where a Safety Authority decrees that it is beyond their ability to manage a Risk within the scope of their delegation, and hence escalation to a higher level is required. This process is mandated for Class A Risks, but is not restricted to such, i.e. the principles and templates can be applied proportionately to any Risks deemed appropriate for escalation.

10.2.3. Wherever possible, the review, agreement, authorisation and acceptance of Risks shall be conducted in-committtee with all relevant stakeholders present. All decisions shall be formally recorded and documented or referenced in the Hazard Log. Where this is not possible and recommendations/decisons need to be communicated between relevant parties, the proforma at Annex I shall be used.

10.3. Process

10.3.1. The process diagram for Risk Acceptance is shown at Figure 6 below.

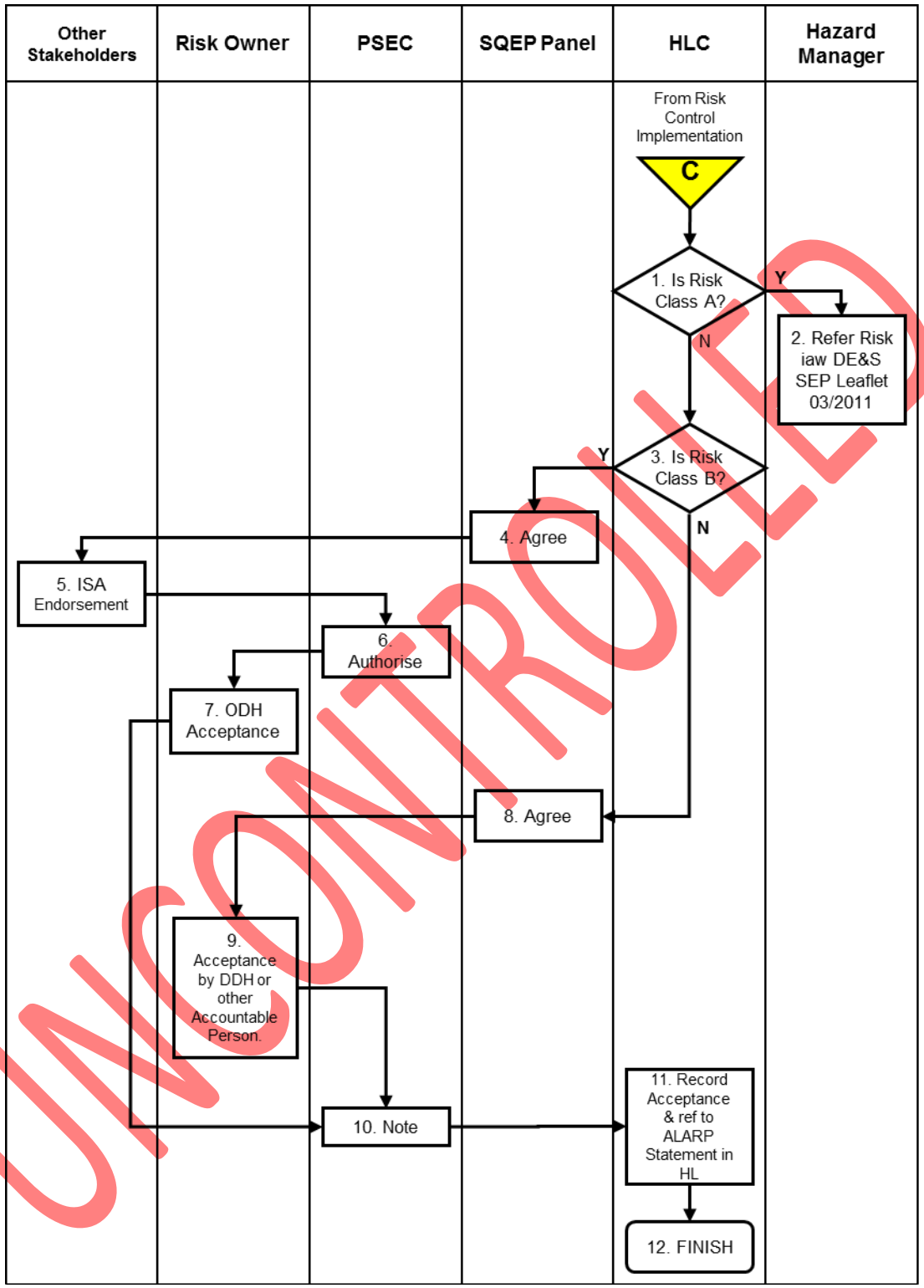


Figure 6 – Risk Acceptance Process

10.4. Process Steps

10.4.1. C - From Risk Control Implementation

10.4.1.1. Risk Acceptance follows Risk Control Implementation, and by the commencement of this activity:

10.4.1.2. The risks in question must be clearly defined, understood, and correctly classified.

10.4.1.3. Risk Control Measures must be clearly articulated, have appropriate owners and assurance must be in place that they have been implemented or, for planned Risk Control Measures, that action plans are in place to implement them within formally agreed and reasonably practicable timescales.

10.4.1.4. ALARP Statements must be in place, proportional to the level of Risk.

10.4.1.5. Whilst the HLC will administer much of this activity, the Hazard Manager will facilitate proceedings to ensure that risks are accepted by, or on behalf of, the relevant Duty Holder or Accountable Person.

10.4.2. Steps 1 and 2 - Decision on Risk Class A Risks

10.4.2.1. Class A risks represent those which are normally regarded as UNACCEPTABLE, but on occasion a Class A risk may need to be tolerated for defined operational benefits. DE&S S&EP Leaflet 03/2011 must be applied in all cases.

10.4.2.2. **Note**: For Equipments/Systems/Platforms in the Design phase, attention is drawn to the following extract from the DE&S Risk Referral Leaflet:

"At the early stages of a project, DE&S hazard analysis and risk assessment activities are likely to identify a number of hazards which will be assessed as presenting a high level of risk until mitigation measures can be shown to be implemented. When the PT sees a reasonable prospect of reducing those risks, it will not need to refer them up the chain of command."

10.4.3. Step 3 - Decision on Risk Class B Risks

10.4.3.1. Class B risks shall be referred to the SQEP Panel for agreement.

10.4.4. Step 4 - SQEP Panel Agreement for Class B Risks

10.4.4.1. For Class B risks, the SQEP panel shall review the adequacy of risk controls and the associated ALARP statement, and make an appropriate recommendation to the PSEC via the ISA.

10.4.5. Step 5 – ISA Endorsement for Class B Risks

10.4.5.1. Following SQEP panel agreement, the Project ISA shall review the adequacy of risk controls and the ALARP Statement, and also confirm that the Risk Assessment meets the requirements of policy, procedures and recognised good practice.

Note: This is deemed to be the minimum requirement for ISA review and, depending on the Equipment/System/Platform in question, the ISA may be requested to review risks other than Class B, e.g. very high consequence risks, risks related to novel technologies, etc.

10.4.6. Step 6 - PSEC Authorisation for Class B Risks

10.4.6.1. The PSEC will review Class B risks and, taking due account of the SQEP Panel and any ISA comments, will authorise the risk for acceptance by the ODH or other 2* Accountable Person.

10.4.7. Step 7 – ODH Acceptance of Class B Risks

10.4.7.1. Class B risks shall be accepted by the ODH or other 2* Accountable Person.

10.4.8. Step 8 - SQEP Panel Agreement for Class C and Class D Risks

10.4.8.1. For Class C and Class D risks, the SQEP Panel shall review the adequacy of risk controls and the associated ALARP Statement and make an appropriate recommendation to the Delivery Duty Holder or other Accountable Person for their review and acceptance.

10.4.9. Step 9 - Acceptance of Class C and Class D Risks

10.4.9.1. Class C Risks shall be accepted by the DDH or other 1*/OF5 Accountable Person.

10.4.9.2. Class D Risks shall be accepted by the relevant Accountable Person.

10.4.10. Step 10 - PSEC Note Risk Acceptance Decision

10.4.10.1. All risk acceptance shall be notified to the PSEC. For higher level risks, it may be appropriate to do this out of committee, as and when risk acceptance takes place. Whereas for lower level risks, it will likely be more appropriate to provide a summary report/update at scheduled PSEC meetings.

10.4.11. Step 11 - Record Acceptance in Hazard Log

10.4.11.1. All risk acceptance decisions shall be recorded in the Hazard Log by the HLC. Importantly, it is essential that the associated approved ALARP Statement (or reference to it) is also included.

10.4.12. Step 12 - Finish

10.4.12.1. At this point the process is concluded. ALARP risks shall be subject to review under the Routine Risk Review activity (Stage 6) process, with review periodicity according to Risk Class.

10.5. Guidance

10.5.1. All safety risk for in-service vessels is ultimately owned by the relevant Duty Holder or other Acountable Person, and risks can only be accepted by them or on their behalf by a suitably empowered representative. The acceptance of risk implies both that risk controls are in place to reduce the risk to ALARP, and that the residual risk level is tolerable in the context of the operational or other benefits to be gained.

10.5.2. Those responsible for recommending and/or endorsing risks for acceptance must satisfy themselves that:

10.5.2.1. All mandatory and Reasonably Practicable risk controls are in place

10.5.2.2. The ALARP and Tolerability justification is sufficiently robust

10.5.2.3. The ALARP Statement provides a clear, unambiguous argument as to why the Risk is considered to be ALARP and Tolerable

10.5.2.4. The appropriate Accident descriptor has been assigned in accordance with Table 1 below

10.5.2.5. As per Table 2 below, a Review Date been assigned appropriate to the Accident Descriptor and Risk Classification.

10.5.2.6. Risks are being referred to the correct Duty Holder or other Accountable Person for acceptance.

10.5.3. ALARP and Tolerability Justification

10.5.3.1. The definitive DE&S guidance on ALARP is DE&S S&EP Leaflet 02/2011 – *ALARP in a Military Equipment Capability Context*. Importantly, it recognises that in the military context:

1) It may be necessary for the ALARP judgement to take account of the operational imperative;

2) Planned action to reduce a Risk over time does not prevent it being declared ALARP, provided that the Residual Risk throughout is deemed tolerable and actions are completed to agreed timescales.

10.5.3.2. The overriding principle is that **"EQUIPMENT MUST NOT BE OPERATED WITH RISKS THAT HAVE NOT BEEN FORMALLY ASSESSED, JUSTIFIED AND DECLARED TO BE ALARP AND TOLERABLE"**.

10.5.3.3. Those involved in making ALARP recommendations must refer to the S&EP Leaflet as necessary, in order to satisfy themselves that the Duty Holder or Accountable Person is able to declare that:

1) The Risk can be declared ALARP and Tolerable;

or;

2) The Risk is not deemed ALARP and Tolerable and action is required to limit/cease (or not undertake) the associated activity.

10.5.4. ALARP Statements

10.5.4.1. Every risk must have an associated ALARP Statement; this is the reasoned argument that all reasonable steps have been taken to ensure that risk is ALARP and Tolerable.

10.5.4.2. The basis and size of the ALARP statement is proportionate to the Risk. More effort and justification will go into class A and B risks than into Class C risks. Class D risks are considered to be Broadly Acceptable and therefore a simple summary ALARP statement that confirms legal/regulatory obligations have been met and suitable good practice was applied may be sufficient.

10.5.4.3. It is important to emphasise that the ALARP Statement is a summary of the ALARP justification, and does not need to duplicate specific evidence from the body of the Hazard Log. For example, it is acceptable to say that "Relevant Good Practice has been identified and applied" in the ALARP Statement, provided that the specific evidence to substantiate this is contained within the Control Measure section of the Hazard Log.

10.5.4.4. Annex G provides guidance on the composition and amount of substantiation required to demonstrate ALARP. **Note:** This is only guidance and should be tailored to the specific risk.

10.5.5. Risk Status

10.5.5.1. All risks shall have an Accident descriptor assigned in accordance with Table 1 below.

eCassandra Accident Descriptor	Definitions	ALARP Status
DRAFT	• Accidents may be entered into the Hazard Log at DRAFT status during the information capture stage.	**NOT ALARP**
OPEN	• Hazard identified, initial risk estimation made, recorded in the Hazard Log and appropriate governance action initiated. • Risk has an ALARP Statement waiting for Endorsement (see para 10.5.3.2 above). • Risk which has been identified for transfer to another authority. • Risk declared NOT ALARP and related activity ceased pending resolution.	**NOT ALARP**
MANAGED	• Risk Owner (or an empowered representative) has accepted that the Hazard is controlled and the risk is ALARP and Tolerable at this time, but a programme, formally agreed by the Duty Holder or Accountable Person, is in place to implement additional specific Reasonably Practicable risk control measures to further reduce the risk level. All agreements shall be recorded in the Hazard Log. • The status of planned risk control measures for MANAGED risks is reviewed on a monthly basis during Director Ships Support's hold to account meetings with the 1* Delivery Heads - Delivery Teams are required to provide updates via the relevant Programme Management Office (PMO) accordingly.	**ALARP**
ACCEPTED	• To be used in exceptional circumstances only, where for operational imperative a Risk Owner chooses to accept a non-ALARP risk.	**NOT ALARP**
ALARP	• Risk Owner (or empowered representative) has accepted that the Hazard is controlled and risk is ALARP and Tolerable. • Notwithstanding routine review activities, no further action is required.	**ALARP**
DELETED	• Risk has been transferred to and accepted by another authority. • Hazard eliminated • Risk assessed as Not Credible • Hazard/Risk duplicated • Hazard now superseded by a new assessment. • Risk has been archived. Archived risks must be endorsed by the relevant delegated authority, with a clear explanation as to why they have been archived.	**NOT APPLICABLE**

Table 1 – Risk Status Definitions

10.5.6. Risk Review Date

10.5.6.1. The review periodicity for individual Risks needs to be proportionate, and will therefore be dependent on the Accident Descriptor and Risk Classification. Whilst there are no mandated arrangements within the Maritime Domain, Table 2 below is intended to offer some guidance on proportionate timescales for actioning/reviewing Risks.

10.5.6.2. Note: The suggested timescales below relate to routine review activity to ensure that plans remain on-track. As per the guidance for Stage 4 (Implementation of Risk Controls), for MANAGED risks where there are additional risk control measures planned, it is expected that review mechanisms will be in place to ensure timely implementation.

eCassandra Accident Descriptor	Risk Classification	Suggested Action/Review Timescale
OPEN	UNCLASSIFIED	Immediately if User Exposed to Risk (see para 10.5.3.2 above)
	A	
	B	
	C	
	D	
MANAGED	A	Weekly
	B	Monthly
	C	Quarterly
	D	Annually
ACCEPTED	A	Weekly
	B	Monthly
	C	Quarterly
	D	Annually
ALARP	A	Quarterly
	B	At least Annually
	C	2 to 3 years depending on Consequence
	D	3 to 5 years depending on Consequence
DELETED	UNCLASSIFIED	N/A – for reference if required
	A	N/A – for reference if required
	B	N/A – for reference if required
	C	N/A – for reference if required
	D	N/A – for reference if required

Table 2 – Guidance on Risk Review/Action Timescales

10.5.7. Risk Acceptance Levels

10.5.7.1. Class A Risk to Life (RtL)[14] shall be managed in accordance with the DE&S Safety and Environmental Protection Leaflet 03/2011 - "Equipment Safety Risk Referral".

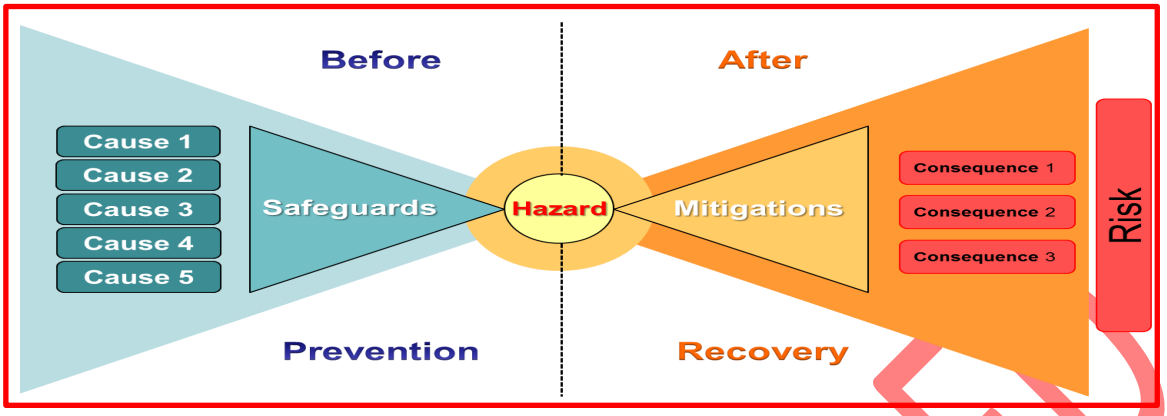
10.5.7.2. Class B RtL shall be formally accepted by the Operating Duty Holder or other 2* Acountable Person.

10.5.7.3. Class C RtL shall be formally accepted by the Delivery Duty Holder or other 1*/OF5 Accountable Person.

10.5.7.4. All other Risks shall be formally accepted by the relevant Accountable Person.

[14] As per Section 4, Risk to Life includes those risks where the Consequence Definition from the SHIPS Common Risk Classification Matrix is Major or worse.

11. STAGE 6 – RISK REVIEW



11.1. Key Safety Outcomes

11.1.1. The outcomes of this stage are: regularly reviewed Hazard Logs; assurance that risks are being reviewed at a frequency appropriate to their significance, and; the initiation of risk reduction actions where warranted by changes in circumstances.

11.2. Introduction

11.2.1. It is expected that risks with an Accident Descriptor of OPEN or MANAGED will be subject to review at each SQEP Panel meeting, unless a clear rationale is recorded for extending the review interval. Accordingly, the process and guidance in this section applies to the routine review of risks whose Accident Descriptor is ALARP.

11.2.2. In principle, all risks are open to further risk reduction measures where these are 'Reasonably Practicable'. Experience of operating a system may suggest that risks are higher than initially assessed, or changes in technology may make possible risk controls which were not previously practicable. Planned system modifications or new equipment fits may also present opportunities to reduce or eliminate long-standing hazards/risks. All of these reasons provide rationale for periodic review of risks which may otherwise be regarded as ALARP.

11.2.3. The frequency of, and effort applied to, such review must be proportionate to the level of risk. O&A Statements and/or SEMPs shall define the risk review criteria to be followed. As per Table 2 in Stage 5 (Risk Acceptance) of this Leaflet, the following frequency of risk review is proposed:

11.2.3.1. Class A - Quarterly;

11.2.3.2. Class B - At least annually ;

11.2.3.3. Class C – Between two and three years, depending on Consequence;

11.2.3.4. Class D - Between three and five years, depending on Consequence.

11.2.4. In addition to reviewing entries in the Hazard Log, safety risks arising from the integration of equipments/systems into platforms shall also be subject to review. PAs shall maintain a record of all equipments/systems fitted to Platforms for which they have responsibility, and shall initiate a safety review of each interface at least annually. Such reviews must be proportionate to the safety significance of the equipment/system and the interface, but shall be formally conducted and recorded, addressing at least the following:

11.2.4.1. Status of equipment/system hazards/risks, safety reports and outstanding risk reduction actions;

11.2.4.2. Operational feedback, including any incidents/safety reports;

11.2.4.3. Any intended modifications which may affect the safety interface.

11.2.5. The relevant risk owners shall be represented, and a record of the review, topics considered and actions taken shall be recorded. Safety risk actions shall be monitored by the appropriate SQEP Panel(s).

Process

11.2.6. The process diagram for Risk Review is shown at Figure 7 below.

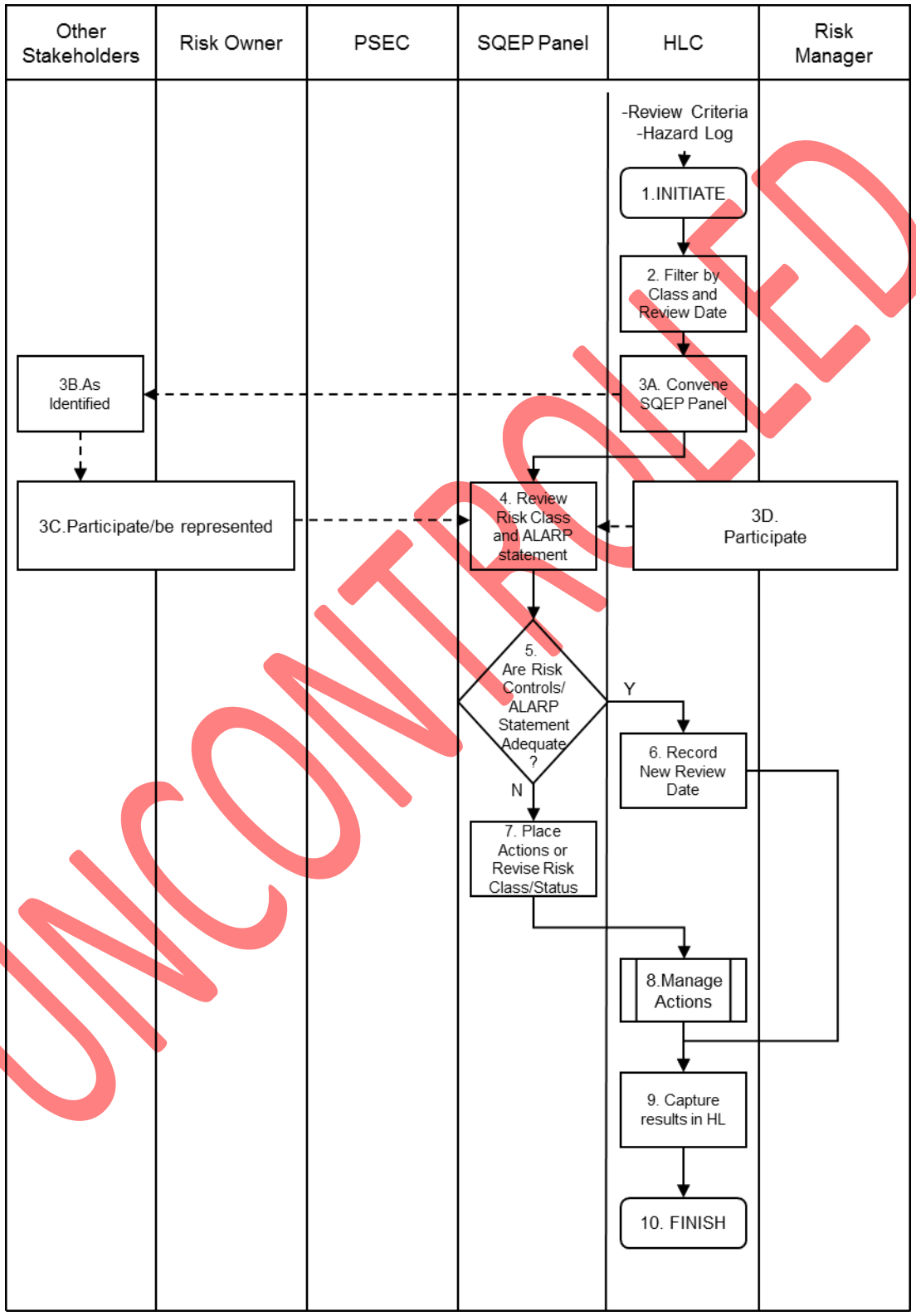


Figure 7 – Risk Review Process

11.3. Process Steps

11.3.1. Step 1 - Initiation

11.3.1.1. The HLC shall ensure alignment between the expected frequency and duration of SQEP panel meetings and the number of risks requiring review according to their Classification. It is assumed that once this is done, the calendar of Panel meetings will drive the identification of risks requiring review before the subsequent meetings. Risk Review is likely to be only one agenda item, with review of OPEN and 'MANAGED' risks also usually being conducted.

11.3.2. Step 2 - Filter by Classification and Review Date

11.3.2.1. In preparation for each SQEP Panel, the HLC shall filter the Hazard Log for all risks due for review in accordance with the review criteria in the O&A statement/SEMP.

11.3.3. Step 3 - Convene SQEP Panel

11.3.3.1. A suitable SQEP panel must be selected to cover the risks under consideration, and SQEP panel members provided with relevant information for pre-meeting review, e.g. summary report, accident/incident information, details of any known modifications, etc.

11.3.4. Step 4 - Review Risk Classification and ALARP Statement

11.3.4.1. Review of risks must be proportionate to their classification. The following questions should guide the review of each risk:

1) Is the risk and ALARP statement clearly expressed?
2) Have any events/incidents occurred which challenge the basis of the risk assessment?
3) Have operating patterns changed in a way that increases or decreases risk?
4) Does technology offer any new ways of controlling/reducing risk?
5) Are any modifications planned to the equipment/system/platform which offer an opportunity for risk reduction?

11.3.5. Step 5 - Decision on the Adequacy of Risk Controls

11.3.5.1. If the Risk Review identifies any potential additional risk control measure, the requirement to implement them or otherwise shall be considered in accordance with the direction and guidance at Stage 4 (Implementing Risk Control Measures) of this Leaflet.

11.3.6. Step 6 - Record new Risk Review Date

11.3.6.1. The completion of a risk review must be recorded in the HL with a summary of actions, and this shall trigger a new review date in accordance with the Risk Classification and Accident Descriptor (see Stage 5 – Risk Acceptance), noting that either or both may have changed as a result of the risk review.

11.3.7. Step 7 - Place Actions/Revise Risk Classification/Status

11.3.7.1. Any necessary actions shall be recorded using the appropriate tool. Where significant actions are required, consideration must be given to changing the Accident Descriptor from ALARP to OPEN or MANAGED.

11.3.8. Step 8 - Manage Actions

11.3.8.1. Actions must be managed with priority according to safety significance.

11.3.9. Step 9 - Capture results in HL

11.3.9.1. Overall completion of the risk review shall be summarised in the Hazard Log.

11.3.10. Step 10 - Finish

11.4. Guidance

11.4.1. Once risks have been accepted as ALARP, it is important that they are not forgotten. Although at the time they were accepted, a decision was made, implicit in the ALARP judgement, that the cost (in time, trouble, operational capability and financial terms) of any further risk reduction measures was Grossly Disproportionate to any risk reduction effected; this balance may change over time. New technologies may become available which enable risk reduction at lower cost; other update requirements may make measures practicable which previously were not; or assessed risk levels may change as a result of operating experience and feedback.

11.4.2. There is therefore a need for a systematic approach to review of risks which have been accepted as ALARP. Such review must be at a periodicity proportionate to the Classification of risks. Risk review sessions held around quarterly and taking a suitable proportion of risks for review may be more effective than longer and less frequent reviews. Where teams have a large number of Class C risks, a distinction should be made between those with a consequence of Critical or above and the rest. Higher potential consequence always deserves closer scrutiny to ensure that assessment of probability is soundly based.

11.4.3. Risk review provides an opportunity, if suitably led, for collective thinking about risk and for reinforcement of safety culture. User input and an element of independent challenge are both essential for maximum benefit. The frequencies of review recommended are such that with normal turnover of people in a project team, risk reviews must enable risks to be retained in the collective memory in order to maintain awareness and influence other routine activities.

11.4.4. Prior to conducting a risk review, consideration must be given to:

11.4.4.1. Review of operating history;

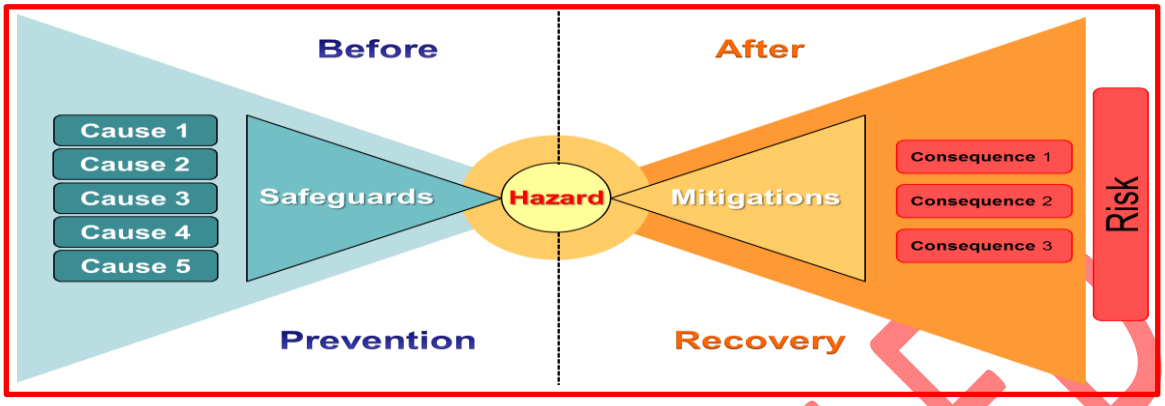
11.4.4.2. Review of any legislative or policy changes affecting risk assessment;

11.4.4.3. SQEP attendance;

11.4.4.4. User representation;

11.4.4.5. Independent challenge (e.g. ISA or another Project team).

12. HAZARD LOG MANAGEMENT



KEY RELATED DOCUMENTS

- DE&S guidance on Hazard Log management is contained within POSMS Safety Management Procedure SMP11

12.1. Key Safety Outcomes

12.1.1. The outcome of this stage is a Hazard Log which supports effective safety management by enabling prioritisation of effort, providing current status of hazards and risks, and provides a full audit trail to support change programmes and audit/assurance.

12.1.2. Each Platform/System/Equipment Authority shall maintain a Hazard Log providing a full record of safety risks under their management.

12.1.3. All authorised stakeholders should be able to obtain read-only access to the Hazard Log, but addition and editing of entries shall be carefully controlled. This may be achieved by a nominated Hazard Log Coordinator (HLC) who shall operate in accordance with defined processes so that changes of risk status and decisions are fully accounted for. The HLC serves as a single point of entry/change.

12.2. Requirements

12.2.1. Table 3 below outlines the high level Hazard Log Management requirements for the various stages of the End-to-End Risk Management Process.

Activity	Requirements
Hazard Identification	• Capture Hazards at earliest stages • Enable multiple HAZID activities • Record/link to HAZID activity records • Enable both Title and Description • Identify applicable equipment/system/platform • Identify Hazard Manager
Risk Analysis and Assessment	• Enable use of Ships OC RCM • Record assessment of Consequence and Likelihood • Identification of Key Safety Functions affected • Identification of DLOD dependencies
Generating Options for Risk Control	• Record options identified
Implementing Risk Control Measures	• Record/link to agreed actions and decision making group • Action tracking to enable action ownership • Capture reasons for options not taken • Capture Risk Status
Risk Acceptance	• Provide prompts on levels of risk acceptance • Record/link to document providing evidence of risk acceptance
Risk Review	• Enable bring-up according to Risk Classification and Review Date • Capture Review date and review outcomes
In Service Support	• Enable read-only access authorised users • Enable comparison of specific Risks/Controls across multiple Hazard Logs • Enable export of risk information in agreed format to Duty Holders
Hazard Log Maintenance/ Meeting support	• Enable sorting according to Risk Status • Enable sorting according to Risk Classification • Enable searching for key words • Enable archiving of risks which are retired, superseded, or consolidated • Link to, or provide facility for, Risk Action tracking • Maintain audit trail of changes to HL • Enable transfer of Hazard Manager

Table 3 – High Level Requirements for Hazard Log Management

12.3. Hazard Log Rationalisation

12.3.1. The High Level Hazard Management Process for Rationalised Hazard Logs is described at Annex H.

12.4. eCassandra Hazard Log Tool

12.4.1. Specific guidance on the eCassandra Hazard Log Tool is contained within a SEP Technical Note, accessible via the Ships Domain Safety & Environmental Page.

ANNEX A – SQEP FORM

Suitably Qualified & Experienced Personnel (SQEP) Proforma						
[Meeting Title]						
Attendee's Name						
Organisation						
Position						
Responsibilities						
Telephone No.			**Fax No.**			
E-mail						
Postal Address						
Qualifications						
Role [please tick appropriate box(es)]	**Operation**		**Maintenance**		**Design**	
	Project		**Safety**		**Other (please specify below)**	
Relevant Experience						
Attendee's Signature						
Chairman's Signature						

General Data Protection Regulations

The GDPR (EU 2016/679) affords greater protection and control of your personal data. As such, information captured in this SQEP Form constitutes Personal Data and requires conscious consent by the owner. We would be grateful if you would consider giving your consent below.

The information provided on this form will be stored on a secure file server and will be used, as required, to validate the conduct and level of expertise involved in the Project Safety Committee.

☐ I consent to my personal data being used in accordance with the above provisions.

ANNEX B – HAZARD CAPTURE FORM

Originator:	
Unique ID:	
Equipment:	
System:	
Platform(s):	
Hazard Description:	
Potential Causes:	
Potential Accident Consequences:	

Existing Risk Control Measures	

Recommended Additional Control Measures	
Risk Control Measure	**DLOD Owner**

ANNEX C - HAZARD COMMUNICATION PROCESS

C.1. Definitions

C.1.1. This process uses three key definitions:

C.1.1.1. **Export Team**. The Authority responsible for communicating identified hazards to the appropriate Importing Authority.

C.1.1.2. **Import Team.** The Authority responsible for accepting Hazards from the Exporting authority and undertaking the necessary risk management activities.

C.1.1.3. **Hazard Communication.** The process by which the Export Team communicates hazards to the Import Team to undertake risk management and the Import Team feeds back the outcome.

C.2. Purpose

C2.1. The purpose of this process is to define a common, auditable process by which Authorities and Duty Holders can communicate information, to ensure that hazards and their associates risks are being managed by those correctly placed to do so.

C.3. Scope

C.3.1. This process can be used to communicate hazards between DE&S Operating Centres (e.g. from a Weapons OC Equipment Authority to a Ships OC Platform Authority), but is principally intended to facilitate the communication of hazards between Equipment Authorities, Platform Authorities and Duty Holders within the Maritime Domain.

C.3.2. It is important to note that this process is not intended to be used for risk referral/escalation, i.e. where an Authority or Duty Holder decrees that it is beyond their ability to manage or accept a risk within the scope of their delegation. A process for doing this is detailed within DE&S Leaflet 03/2011 [Ref x].

C.3.3. Hazards can only be communicated effectively if the hazard is documented with sufficient detail to allow the Importing Authority to understand the hazard's likelihood and potential consequence severity. It is therefore vitally important that during safety assessments this information is recorded accurately.

C.4. Process

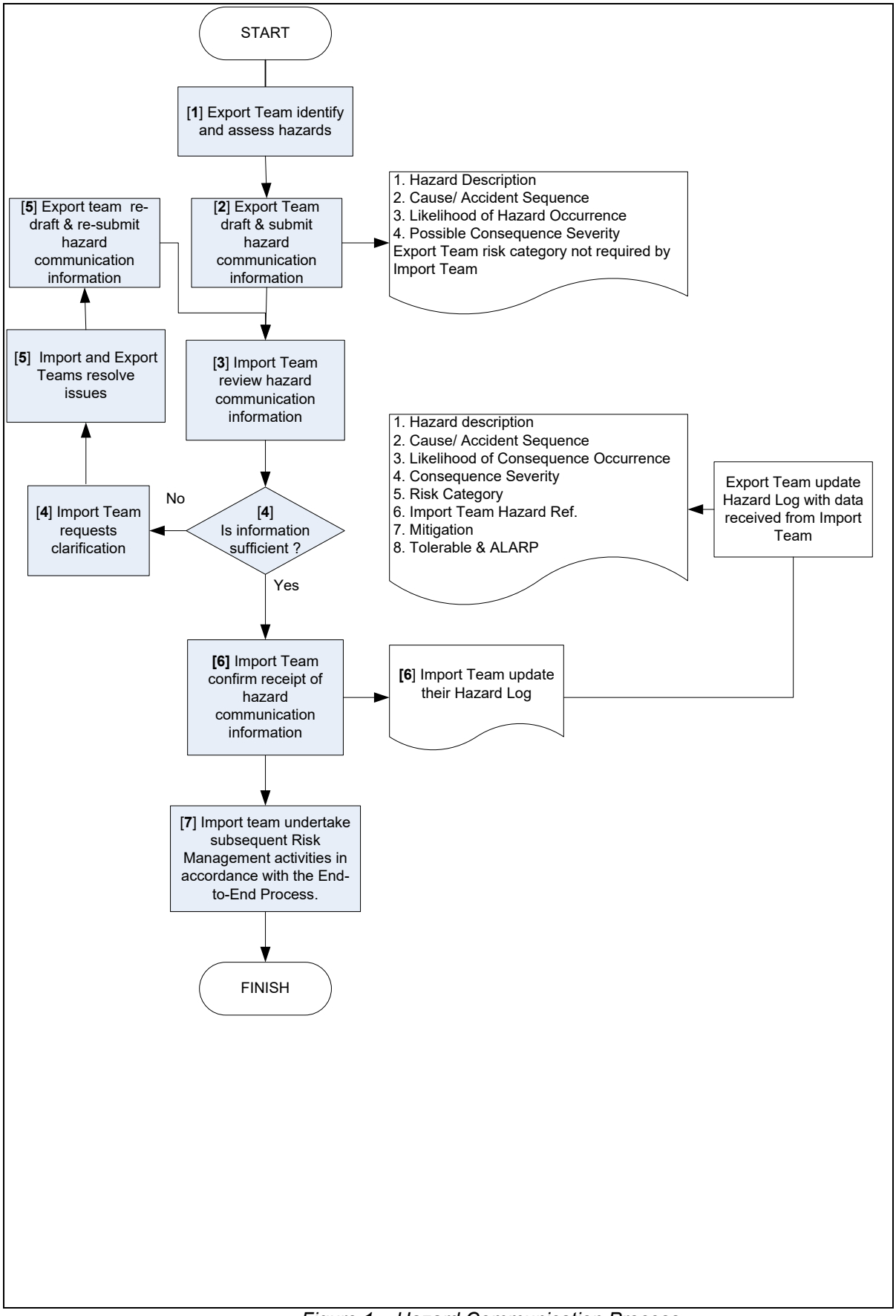


Figure 1 – Hazard Communication Process

C.5. Process Steps

C.5.1. **Step 1.** Where it is identified that a hazard should be managed by a different Authority/Duty Holder, the Export Team is required to contact the appropriate Hazard Manager and inform them of the hazards to be communicated.

C.5.2. **Step 2.** All hazards to be exported must be recorded in sufficient detail, including hazard description, indicative consequence severity and likelihood of occurrence. This information is to be submitted using the Hazard Communication Form at Appendix 1.

C.5.3. **Step 3.** The appropriate Hazard Manager in the Import Team must review the contents of the Hazard Communication Form (and any accompanying documentation) to ensure the information presented is sufficient.

C.5.4. **Step 4.** If the deliverables are not deemed to be sufficiently, they must be returned to the Export Team with a request for clarification. For in-service equipments/systems, the Import Team shall give the Export Team an indication of the priority which for addressing any clarifications.

C.5.5. **Step 5.** As necessary, the respective Hazard Managers must meet to resolve any issues. The Export Team Hazard Manager must then re-work the deliverable as agreed and re-present it to the Import Team.

C.5.6. **Step 6.** If the deliverables are deemed to be sufficient, the Import Team must confirm successful communication with the Export Team. At this point, the Import Team assumes formal responsibility for the hazard and must update their Hazard Log accordingly, i.e. raise a new hazard or update an existing one as appropriate. To record this transfer of responsibility, the Hazard Communication Form must be updated (including appropriate Hazard Log references) and forwarded to the Export Team for their records (copies retained by both parties for audit purposes).

C.5.7. **Step 7.** Once an Import Team has assumed formal responsibility for a hazard, it must be subject to the subsequent risk management activities detailed in the End-to-End Risk Management Process.

APPENDIX 1 TO ANNEX C – HAZARD COMMUNICATION FORM

HAZARD COMMUNICATION REFERENCES	
EXPORT TEAM:	
IMPORT TEAM:	
EXPORT EQUIPMENT/SYSTEM:	
IMPORT SYSTEM/PLATFORM:	
HAZARD COMMUNICATION REF:	
ISSUE NUMBER:	

Proc. Step	EXPORT TEAM HAZARD INFORMATION	Y/ N	Comment
1	Has the content of the communication been derived from the output of a SQEP panel?		
2	Is the following information included and clear in the communication?		
	a) Hazard Description:		
	b) Causes/Accident Sequence(s):		
	c) Likelihood of Accidents(s):		
	d) Potential Consequence Severities:		
	N.B. Resultant Export Team Risk Categories NOT required to be communicated to the Import Team.		
	Export Team Risk Manager Name & Signature:		Date:
3	Is the Hazard information sufficient? (Import Team to confirm):		
	Import Team Hazard Manager Name & Signature:		Date:
6	Has the following information been included in the Import Team Hazard Log?		
	a) Hazard Description:		
	b) Causes/Accident Sequence(s):		
	c) Likelihood of Accident Sequence(s):		
	d) Potential Consequence Severities:		
	Has Hazard Log information been fed back to Export Team?		
	Import Team Hazard Manager Name & Signature:		Date:

ANNEX D - COMMON RISK CLASSIFICATION MATRIX

Risk Classification

A – Intolerable

Can NOT be tolerated – shall not be accepted unless there are exceptional reasons for the activity to take place. Must be managed in accordance with DE&S Safety and Environmental Protection Leaflet 03/2011 – "Equipment Safety Risk Referral".

B – Undesirable

Can be tolerated – A full safety justification and ALARP argument must be provided to justify the risk. Any residual Class B risks shall be autorised by the Project Safety Committee and accepted by the Operating Duty Holder or other 2* Accountable Person.

C – Tolerable

Can be tolerated provided an ALARP status is reached. The record of ALARP status is to be recorded in the Hazard Log. Class C Risks shall be agreed by a SQEP panel and accepted by the Delivery Duty Holder or other 1*/OF5 Accountable Person.

D – Broadly Acceptable

Can be tolerated. A proportional ALARP Statement is to be recorded in the Hazard Log. Class D Risks shall be agreed by a SQEP panel and accepted by the nominated Accountable Person.

Injury and Illness Classifications

Permanent Injury/Illness *Injury/illness from which a full recovery is not possible*	**Recoverable Injury/Illness** *Injury/illness that can be recovered from with medical treatment and recovery time*	**Minor Injury/Illness** *Minor injury/illness requiring basic first aid treatment*
• *Amputation* • *Permanent loss of sight* • *Third degree burns – damage to all layers of skin* • *Major exposure to RADHAZ above threshold level* • *Injury that will lead to permanent disability* • *Permanent deafness* • *Hepatitis* • *Legionellosis*	• *Fractures* • *Sprains* • *Major cuts requiring hospitalisation but recoverable* • *Crush injuries requiring hospitalisation but recoverable* • *Dislocation of the shoulder, hip, knee or spine not resulting in permanent disability* • *Second degree burns – redness, blistering & acute pain* • *Scalds* • *Injury leading to hypothermia, heat-induced illness or unconsciousness or requiring resuscitation or admittance to sick-bay for more than 24 hours* • *Injury resulting from an electric shock leading to unconsciousness or requiring resuscitation or admittance to sick-bay for more than 24 hours* • *Chemical or hot metal burn to the eye or any penetrating injury to the eye not leading to permanent loss of sight* • *Frostbite not leading to amputation* • *Food poisoning leading to admittance to sick-bay for more than 24 hours* • *Smoke inhalation leading to admittance to sick-bay for more than 24 hours* • *Minor hearing loss requiring hearing correction/Tinnitus (ringing in the ears)* • *Minor exposure to RADHAZ above threshold level* • *Acute illness requiring medical treatment, or loss of consciousness arising from absorption of any substance by inhalation, ingestion or through the skin* • *Unconsciousness caused by asphyxia or exposure to a harmful substance or biological agent* • *Dermatitis* • *Acute illness requiring medical treatment where there is reason to believe that this resulted from exposure to biological agent or its toxins or infected material*	• *Cuts* • *Bruises* • *Abrasions* • *Temporary eye irritation* • *First degree burns – redness, sensitivity to the touch* • *Minor electric shock not resulting in unconsciousness* • *Chemical fume inhalation not resulting in unconsciousness*

			Consequence Definition					
			More than 100 deaths	10 to 100 Deaths	1 to 10 deaths	Permanent Injury/Illness	Recoverable Injury/Illness	Minor Injury/Illness
Frequency Definition	**Accident Frequency**	**Accident Frequency per Annum to Group at most risk**	**Catastrophic**	**Disastrous**	**Critical**	**Major**	**Marginal**	**Negligible**
Likely to occur repeatedly on the ship during its life.	**Frequent**	$>10^{-1}$	**A**	**A**	**A**	**A**	**A**	**C**
Likely to occur from time to time on the ship during its life.	**Probable**	$10^{-1} – 10^{-2}$	**A**	**A**	**A**	**A**	**B**	**C**
May occur once on the ship during its life.	**Occasional**	$10^{-2} – 10^{-3}$	**A**	**A**	**A**	**B**	**C**	**D**
Unlikely to occur on the ship during its life.	**Remote**	$10^{-3} – 10^{-4}$	**A**	**A**	**B**	**C**	**C**	**D**
Very unlikely to occur on the ship during its life.	**Improbable**	$10^{-4} – 10^{-5}$	**A**	**B**	**C**	**C**	**D**	**D**
Extremely unlikely to occur on the ship during its life.	**Highly Improbable**	$10^{-5} – 10^{-6}$	**B**	**C**	**C**	**D**	**D**	**D**
Extremely rare event.	**Incredible**	$<10^{-6}$	**C**	**D**	**D**	**D**	**D**	**D**

ANNEX E – GUIDANCE ON COST BENEFIT ANALYSIS

E.1 Cost Benefit Analysis (CBA)

E.1.1 CBA is a defined methodology for valuing costs and benefits that enables broad comparisons to be made between health and safety risk reduction measures on a consistent basis, giving a measure of transparency to the decision making process. In a CBA, all costs and benefits are expressed in a common currency, usually money, so that a comparison can be made between different options[15].

E.1.2. Something is "reasonably practicable" unless its costs are grossly disproportionate to the benefits. Put simply if **Costs > Benefits X Gross Disproportion Factor (GDF)** then it is not reasonably practicable.

E.1.3. Whilst CBA is a useful method in determining which risk reduction measures to implement, it has its limitations, staff should remember the following:

E.1.3.1. A CBA cannot be used to argue against the implementation of relevant good practice, unless the alternative measures are demonstrated unequivocally to be at least as effective.

E.1.3.2. The depth of analysis must be fit for purpose, i.e. more rigour is required where the risk is higher or the consequences themselves are great e.g. multiple fatalities.

E.1.3.3. A sensitivity analysis is usually required to support any conclusions suggesting that the costs are disproportionate to benefits of implementing a measure.

E.1.4. A CBA on its own;

E.1.4.1 Does not constitute an ALARP case.

E.1.4.2 Cannot be used to argue against statutory duties.

E.1.4.3. Cannot justify risks that are intolerable, or justify what is evidently poor engineering.

E.1.5. A CBA tool is available to support staff in undertaking CBA, however it is important to understand the underlying assumptions described in this document in order to be aware of the limitations of conducting CBA.

E.2. Costs

E.2.1. There are many different costs associated with implementing a risk reduction measure, most of these are obvious, but there are many that are less so, the following is a list to aid in identifying these costs:

E.2.1.1. Design Feature

E.2.1.1.1. Design of control measure.

E.2.1.1.2. Installation of control measure.

E.2.1.1.3. Extra training for operators or maintainers.

E.2.1.1.4. Any additional maintenance of control measure.

E.2.1.1.5. Update of documentation (BRs, UMMS, IPCs, etc.).

E.2.1.2. Procedural Control

E.2.1.2.1. Additional training with the procedure.

E.2.1.2.2. Rewriting the procedure.

E.2.1.2.2 Additional staff required.

E.2.1.3. Maintenance

E.2.1.3.1. Rewrite the maintenance procedure.

[15] HSE Principals for Cost Benefit Analysis in support of ALARP decisions

E.2.1.3.2. Additional staff required.

E.2.1.3.3. Additional spares required.

E.2.1.4. Training and Awareness

E.2.1.4.1. Costs of delivering the training.

E.2.1.4.2. Additional staff required.

E.2.1.5. PPE

E.2.1.5.1. Costs of purchase of PPE.

E.2.1.5.2. Additional training.

E.2.2. Any savings as a result of the measure (e.g. avoidance of damage and reinstatement costs if relevant) should be offset against the above costs. These are not considered safety benefits but are counted as 'cost savings' i.e. they reduce the overall cost of implementing a measure.

E.3. Benefits

E.3.1. It is important that all benefits of implementing a health and safety improvement measure are included and that the benefits associated with the measure are not underestimated in any way.

E.3.2. The benefits should include all reduction in risk to members of the public, workers and the wider community. i.e. benefits can be broken down into prevented:

E.3.2.1. Fatalities.

E.3.2.2. Injuries (major to minor).

E.3.2.3. Ill health.

E.3.3. Benefits can include avoidance of deployment of emergency services and avoidance of countermeasures such as evacuation and post accident decontamination if appropriate.

E.3.4. All benefits of a control measure should be included. If a risk reduction control measure is identified for one type of accident but reduces other risks as well e.g. health risks, all benefits should be counted.

E.3.5. It should be noted that duty holders might need to treat re-instatement costs as a benefit rather than offsetting them against costs, this can represent a bias in favour of safety. This is because the gross disproportion factor is applied to all benefits prior to them being compared to the costs.

E.3.6. A risk reduction measure may not eliminate the hazard completely and should only consider the benefit as the amount of reduction of risk, although for simple calculations where the risk is reduced by more than two orders of magnitude it may be assumed that the risk is eliminated.

E.4. Value To Prevent A Fatality (VPF) And Value To Prevent An Injury (VPI)

E.4.1. R2P2[16] introduced the concept of Value to Prevent a Fatality (VPF) for attributing a sum of money to the reduction in probability of a fatality from a hazardous event. There is no central Departmental policy on the figure to be used so, based on the Department for Transport (DfT) published figure for 2007[17], the Ships Board directed in 2009 that a VPF of £2M should be used to calculate the proportionate cost of a risk reduction option. Similarly scaled figures for Value to Prevent an Injury (VPI) are shown in Table E1 below.

Level of Harm	VPF / VPI[18]
Individual Death resulting from accident	£2,000,000
Individual Permanent Injury	£200,000
Individual Recoverable Injury	£20,000
Individual Minor Injury	£2,000

Table E1 – Ships OC Figures for VPF and VPI

E.4.2. To quantify gross disproportion in CBA, a factor must be applied to the total benefit; this is called the Gross Disproportion Factor. This factor is proportional to the Risk Classification, it can be found in Table 2 below.

Risk Class	GDF	Cost factor to justify not making the safety improvement
Class A	10	If the cost exceeds **10 times** the benefit and time the user is exposed to the hazard, the sacrifice is judged to be grossly disproportionate to the benefit gained, but only acceptable where exceptional circumstances demand the capability and the risk has been appropriately referred upwards.
Class B	6	If the cost exceeds **6 times** the benefit and time the user is exposed to the hazard, the sacrifice is judged to be grossly disproportionate to the benefit gained.
Upper Class C	4	If the cost exceeds **4 times** the benefit and time the user is exposed to the hazard, the sacrifice is judged to be grossly disproportionate to the benefit gained.
Lower Class C	2	If the cost exceeds **2 times** the benefit and time the user is exposed to the hazard, the sacrifice is judged to be grossly disproportionate to the benefit gained.
Class D	1	If the cost exceeds the benefit and time the user is exposed to the hazard, the sacrifice is judged to be grossly disproportionate to the benefit gained.

Table 2 - Gross Disproportion Factor

[16] Reducing Risks, Protecting People – HSE's decision-making process.

[17] DfT is considering a study to examine an uplift in their values, but this will not report for some time. Past tracking indicates only a very gradual increase with inflation etc over the last 20 years. Given that the Ships figure is already slightly higher than that of the DfT, it is considered that £2m VPF remains valid.

[18] Values of VPI have been scaled from DfT published figures for 2007. The scaling factor used is D Ships VPF/DfT VPF = £2,000,000 / £1,876,830 = 1.065627. DfT VPI for Serious Injury is set at £215,170 (assumed equivalent to permanent RIDDOR), Slight Injury is set at £22,230 (assumed equivalent to Recoverable RIDDOR) and Damage Only is set at £ 1,970 (assumed equivalent to Non-RIDDOR injury).

E.5. Other Factors

E.5.1. There are a number of features within an analysis that can have influence on the outcome. The following points shall be considered when assessing the suitability of CBA[19]:

E.5.1.1. Discounting of monetary values to translate future benefits/costs to present values is permitted. If there are significant future costs, discounting must be considered to see if this might change the outcome of a finely balanced analysis. Further guidance on discounting can be found in the HSE CBA checklist.

E.5.1.2. The analysis shall be shown to be robust by appropriate **sensitivity analyses**, in line with the precautionary approach. In particular, the results of any CBA associated with major accident hazards will be subject to uncertainty owing to the need to estimate how severe and how often the accidents might be. By their nature, these accidents are rare but when they do happen, they can have very high consequences.

E.5.1.3. Deciding whether or not to implement a control measure is often not as simple as purely looking at the factors involved in CBA. There are many other hidden benefits and costs, such as damage to reputation which need to be considered.

E.5.1.4. Affordability is **not** a legitimate factor in considering costs.

E.5.1.5. The projected use or remaining life of a system or facility must be taken into account.

E.6. Calculations

E.6.1. Calculating gross disproportion:

E.6.1.1. Costs > Benefits X GDF;

E.6.2. Calculating Benefits;

E.6.2.1. Frequency of occurrence x VPF = Annual Benefit;

E.6.2.2. Frequency of occurrence x VPI = Annual Benefit;

E.6.2.3. Annual Benefit x Life Remaining = Lifetime Benefit.

E.6.3. A worked example is at Appendix 1 overleaf.

E.7. Recording Assessments

E.7.1. Where CBA results in the conclusion that a potential Risk Control Measure is Grossly Disproportionate, this must be summarised and referenced in the relevant ALARP Statement(s).

[19] HSE (Extracted 02/08/2011) Cost Benefit Analysis Checklist (http://www.hse.gov.uk/risk/theory/alarpcheck.htm#footnotes)

APPENDIX 1 TO ANNEX E – CBA EXAMPLE

E.8. CBA Example

E.8.1. A hazard exists that an amphibious platform's davit could have a structural failure whilst lifting a landing craft, this could result in the consequence of 1 death, 10 permanent injuries, and 20 minor injuries.

E.8.8.1 From the D Ships RCM this means the consequence is "**Critical**".

E.8.1.2. The annual frequency of occurrence of this accident is qualitatively assessed as being no better than 1 in 10000 years but no worse than 1 in 1000 years. From D Ships RCM this is "**Remote**".

E.8.1.3. Therefore, the risk is assessed as being **Class B** and is therefore in the undesirable range, which requires a substantive safety assessment to demonstrate that the risk is ALARP and no further reasonably practicable control measures could be applied.

E.8.2. The platform is assumed to have 20 more years of service left before disposal.

E.8.3. The benefits of preventing this accident occurring can be assessed as follows:

E.8.3.1. Frequency of occurrence x VPF (or VPI) = Annual Benefit

E.8.3.2. Annual Benefit x Life Remaining = Lifetime Benefit

E.8.3.4. [(1 X £2,000,000) + (10 X £207,200) + (20 X £20,500)] X 0.001 = £4,482 per annum per platform

E.8.3.5. £4,482 X 20 = £89,640 per platform

E.8.4. To show that any control measure is grossly disproportionate requires:

E.8.4.1. Benefits X GDF < Costs

E.8.5. The GDF for a class B hazard from Table is 6:

E.8.5.1. £4,482 x 6 = £26,892 per annum per platform

E.8.5.2. £89,640 x 6 = £537,840 per platform

E.8.6. In addition to this, the accident would also cause significant damage to the landing craft and the davit itself, the cost of replacing both of these will be £250,000.

E.8.6.1. £26,892 + (250,000 X 0.001) = £27,142 per annum per platform

E.8.6.2. £572,004 + (250,000 X 0.001 X 20) = £542,840 per platform

E.8.7. Therefore any control measure that eliminates the risk, that costs less than £27,142 per annum per platform or less than £542,840 as a one off cost per platform would be deemed to be "reasonably practicable".

E.8.8. In some cases it is likely that a control measure will not totally remove the risk, to calculate the values for a smaller risk reduction the total probability is replaced with the risk reduction. This example demonstrates a reduction in probability from a control measure to Improbable:

E.8.8.1. Probability of occurrence before control measure – Probability after = risk reduction probability

E.8.8.2. 0.001 - 0.0001 = 0.0009

E.8.8.3. [(1 X £2,000,000) + (10 X £207,200) + (20 X £20,500)] X 0.0009 = £4,034 per annum per platform

E.8.8.4. £4,034 X 20 = £80,676 per platform

E.9. Sensitivity Analysis Example

E.9.1. Any assessment, be it quantitative or qualitative, will have some degree of uncertainty about it. This uncertainty is likely to be specific for quantitative analysis but for qualitative analysis can be large and unclear. It is important to understand the impact this uncertainty would have on the analysis, this section gives a simple example of how this technique can be employed.

E.9.2. This simple sensitivity analysis will utilise the same CBA method as above but by varying the original assessments:

E.9.2.1. **Severity** – If an additional 1 person were to die then the cost at which a control measure becomes grossly disproportionate over the life of the platform becomes £782,840, as this assessment assumes multiple permanent injuries it may be realistic that an additional person were to die. Conversely, if no one were to die, this cost becomes £203,560.

E.9.2.2. **Probability** – If the probability of this accident was actually Occasional, the risk would become a category A and the GDF would also increase. This would result in the cost at which the control measure becomes disproportionate becomes £9,014,000 and conversely if it were reduced to improbable the cost would be £38,633.

E.9.2.3. There are other factors such as life of the platform that may also need to be taken into account.

E.9.3. This example shows that the final values are extremely sensitive to even small changes in probability, and particular care must therefore be taken when making decisions based on probabilities derived from qualitative judgement based assessments.

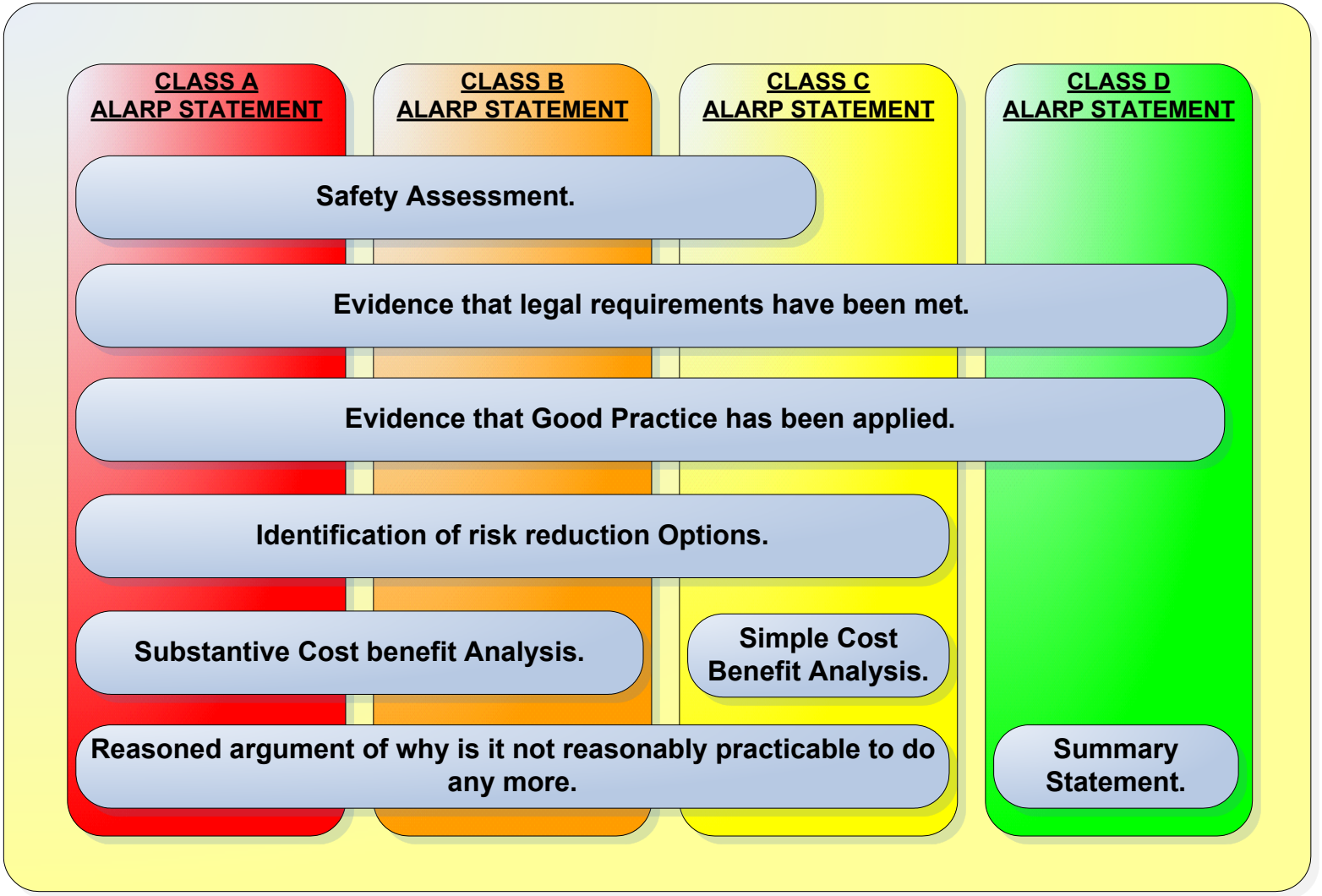
ANNEX F – CLARIFICATION ON THE OWNERSHIP OF RISK CONTROL MEASURES

F.1. Hazard Logs will inevitably contain risks that are mitigated by PA/EA owned risk control measures (e.g. Engineering Design, Operating Instructions, Maintenance Schedules, etc.) and/or other DLOD owned risk control measures (e.g. Navy Command generated Standard Operating Procedures (SOPs), Training, etc.).

F.2. PAs and EAs are ultimately accountable for ensuring that risk control measures provided in support of the 'safe to operate' position are implemented and maintained, providing the Duty Holder or other Accountable Person with confidence that the PA/EA 'safe to operate' judgement is maintained allowing necessary 'operating safely' judgements to be made accordingly. However, it is not the PA/EA responsibility to confirm whether other DLOD owned risk control measures are being realised, i.e. it is not a requirement for the PA/EA to validate that all DLOD owned risk control measures are in place and in date. **Note:** It is important to stress that this advice is intended to clarify the respective PA/EA and other DLOD owner responsibilities for implementing and assuring risk control measures, and is written in the context of the purist PA/EA roles, as described in DSA02-DMR. However, it must be recognised that not only do PAs and EAs **(currently)** chair Platform/Equipment SECs, but importantly from a management perspective, they are also custodians of the Hazard Logs **on behalf of the Duty Holder or other Accountable Person.** Therefore, in this capacity, PAs and EAs **ARE** ultimately accountable for satisfying the Duty Holder or other Accountable Person that **ALL** risk control measures are documented within the Hazard Log, noting however that the responsibility for providing assurance on their implementation lies with the respective control measure owners.

F.3. **Responsibility** for confirming that all risk control measures are managed lies with the nominated **Hazard Manager.** All risk control measures must be fully referenced in the Hazard Log. Those references must include the detail of the source document, and all relevant DLOD owners shall be included/consulted when SQEP panel activities are undertaken. Where risk control measures cannot be validated or where there is doubt over ownership, then clarity must be sought from the appropriate DLOD lead in the first instance. Any remaining ambiguity shall be addressed through the Surface Ship Operating Safety Group in Navy Command. Where such instances arise, the Hazard Manager shall ensure in all cases that the Accident Descriptor is retained at or subsequently changed to OPEN until the situation is resolved.

ANNEX G - ALARP STATEMENT PROPORTIONALITY TO RISK



ALARP STATEMENT PROPORTIONALITY - GUIDANCE

G.1. The diagram above provides guidance on the composition and amount of substantiation required to demonstrate ALARP, this is only guidance and should be tailored to the specific risk. An ALARP statement may consist of:

G.1.1 **Safety Assessment.** Describes the accident sequence and justifies the consequences and the frequency analyses. It would go on to show which individuals are at most risk of being harmed and show the basis of the risk assessment.

G.1.2. **Evidence that Legal Requirements have been met.** Shows that legal obligations have been assessed and complied with, Accountable Persons are obliged to comply with statutory duties regardless of sacrifice. Where MOD is exempt from statutory obligations then the statement needs to show how the Accountable Person has met the Secretary of States policy that "Where Defence can rely on exemptions or derogations from either domestic or international law we introduce standards and management arrangements that are, so far as reasonably practicable, at least as good as those required by legislation."

G.1.3. **Evidence that Good Practice has been applied.** Demonstrates that appropriate "good practice" which includes Approved Codes of Practice, classification society rules, standards, etc. have been applied. If "good practice" is deemed inappropriate then a justification must be provided to argue why it is inappropriate.

G.1.4. **Identification of Risk Reduction Options.** After the application of "good practice" then all feasible further risk reduction measures must be explicitly identified.

G.1.5. **Cost Benefit Analysis (CBA).** This must be proportionate to the class of risk under consideration, further guidance can be found at Annex E.

G.1.6. **Reasoned Argument.** Is a compelling rationale of why no further risk reduction is Reasonably Practicable, supported where necessary by the CBA.

G.1.7. **Summary Statement.** For risk Class D only, a simple statement such that through the application of good practice (quoting source of good practice), the residual risk is assessed as Class D. It must be ensured that the justification for assessment as class D is sufficient, defensible and recorded.

ANNEX H - HIGH LEVEL HAZARD MANAGEMENT PROCESS FOR RATIONALISED HAZARD LOGS

H.1. Introduction

H.1.1. This Annex applies only to rationalised Hazard Logs that have been structured in accordance with the Ships Operating Centres' Safety Function Model (SFM) at Appendix 1. A rationalised Hazard Log approach has been established in order to optimise the management of the quantity of information captured, and to present the hazard and risk information in a structure that provides a better understanding of the Platform risks from a functional perspective. These Hazard Logs have a focused number of hazard records which are referred to as High Level Hazards (HLH), representing the high level Platform hazards.

H.1.2. Rationalised Hazard Logs work on the principle of HLHs that capture numerous accident sequences, therefore working as a 'many-to-many' Hazard Log as opposed to the 'one-to-one' or 'one-to-many' structure previously employed. This approach allows users to identify the risks that require the most effort for risk reduction as well as aiding the identification of any safety risks not previously considered.

H.1.3. The principles of safety risk management at stages 1-6 of this leaflet remain the overarching guidance. Rationalised Hazard Logs differ only in their collation of accident sequences against a central functional hazard. Therefore, management activities described here only complement what has already been described.

H.1.4. Rationalised Hazard Logs will only contain information on the current in-service safety status of the platforms, and will therefore not contain any design/build information unless it is pertinent to an in-service safety risk.

H.2. Rationalised Hazard Log Structure and the Safety Function Model

H.2.1. This structure identifies the typical Safety Functions provided by the vessels supported within the Ships Operating Centres. These functions vary from provision of intrinsic functions, to the ability to cover hazardous activities onboard or to identify and respond to emergency situations. However, not all vessels provide all Safety Functions and not all Equipments or Systems support all the functions, therefore **Platform Teams are required to tailor the rationalised Hazard Log structure for their Platforms.**

H.2.2. The SFM also identifies where Naval Authority Certification is required through capture of the relevant Naval Ship Code Chapter.

H.2.3. The Safety Functions break down from a top level function to 2nd and 3rd level sub-functions, with each having a corresponding title and description to make the function of each sub-function clear to users. HLHs are then 'Failure of…' the corresponding Safety Function. The HLH groups the accident sequences in the bow-tie structure, capturing the various causes, risks, applied mitigations and ongoing actions applicable to that Hazard.

H.2.4. There may be instances where changes are required to the Safety Function Model. Further guidance and a change management process is at Appendix 2.

H.3. Applicability

H.3.1. Use of the eCassandra Hazard Log tool is mandated[20] throughout the life of the Platform, System or Equipment. In order to maintain consistency through-life, the functional approach should be used from the project start at the Concept Phase and used through to Disposal.

H.3.2. CADM – Concept, Assessment, Design and Manufacture

H.3.2.1. During Concept, Assessment, Design and Manufacture phases (or MAID equivalents), Platform Teams who are sub-contracting delivery of Safety Cases shall apply DEFSTAN 00-56 to specify that procurement of new Platforms, Systems or Equipments shall include provision of eCassandra in-service Hazard Logs that are structured in accordance with the Safety Function Model. By structuring Hazard Logs functionally at this stage, Platform Teams can:

[20] DE&S S&EP Leaflet 13/2017 - The DE&S Way for System Safety and System Environmental Protection.

H.3.2.1.1. Assure themselves that the Safety Functional requirements of the Platform can be met;

H.3.2.1.2. Provide a consistent structure for the Hazard Logs throughout the life of the Platforms, thereby minimising the effort required to transfer Hazard and Risk information, particularly at phase handover points;

H.3.2.1.3. Provide a framework that is consistently working towards providing functional safety information for the in-service phase.

H.3.3. In-Service

H.3.3.1. Management of rationalised Hazard Logs at the in-service phase of life includes any periods where Platforms are in Non-Fleet Time, upkeep (extended or otherwise) or extended readiness, as well as when they are operating under Fleet Time.

H.3.4. Disposal

H.3.4.1. At Disposal, vessels do not necessarily need to provide the Safety Functions they were required to in-service and, furthermore, the risk management approach of a ship destined for scrap does not need to be the same as that for a ship destined for a potential foreign sale. Safety Authorities should assess the disposal approach in accordance with POSMS (SMP16) and structure the Disposal Safety Case and Hazard Log accordingly, noting that the new Hazard Logs will supersede the Hazard Log used in-Service.

H.4. Auditability

H.4.1. Although the in-service rationalised Hazard Logs shall have auditable links to build or production Hazard Logs, they will not contain hazards identified during the design, assessment and build phase of the project except where these hazards and risks continue to have an impact on In-service life. The rationalised Hazard Logs will also not include any historical hazard records from the pre-rationalised Hazard Log. It is incumbent upon the Platform Teams to ensure that any previously used Hazard Logs, or their traceability, are available for audit and that the in-Service phase remains the focus for the rationalised Hazard Logs.

H.5. Assignment of Managers to High Level Hazards

H.5.1. The *Key Principles and Responsibilities* Section of this document describes the responsibilities of both the Risk Owner and Hazard Manager. For rationalised Hazard Logs, each HLH will ilkely have multiple risks associated with it; for these risks, the definition of the Hazard Manager described above applies. In addition, each HLH will have a specific HLH manager nominated.

H.5.2. HLH managers shall be identified in the relevant SEMP(s) and must hold a Letter of Safety Delegation in accordance with Leaflet 14 of the SHIPS OCs' S&EP O&A Statement.

H.5.3. The HLH manager is responsible for oversight of the HLH, particularly the upkeep and currency of all associated information, including causes, risks, control measures and actions. Whilst the HLH manager will not be the owner for all records, he/she is responsible for ensuring that records are adequately maintained and updated by the record owner.

H.6. Tailoring

H.6.1. It is the responsibility of the project teams to identify the Safety Functions applicable to their platforms, systems and equipments and capture them appropriately. This capture shall also record the corresponding HLH Manager.

H.6.2. A key benefit of adopting rationalised Hazard Logs is the ability to optimise time spent managing the information, therefore it may be appropriate for some HLHs to cover more than one function, either due to quantity of information available or coherence of mitigation across the function. A good example of this is functions 9.2 and 9.3 for the Radar and Wireless Telegraphy functions, where the risks to life from exposure to both radar and radio emissions are similar; additionally, there is commonality in the control measures applied to these risks on platforms such as the SHIPHAZ management process adopted by Surface Ships.

H.6.3. Once the platform Safety Functions have been determined, it is unlikely that they will change significantly unless the ship undergoes an Alteration & Addition or modification which significantly alters the operating envelope or capability of the platform. Therefore, the platform Safety and Environmental Management Plans (SEMPs) shall map the HLHs to the relevant Safety Functions and ensure this mapping is maintained throughout the in-service life of the platform.

H.7. Management Of System And Equipment Hazards At The Platform Level

H.7.1. Within the Ships OCs, the Platform Authorities (PAs) are responsible for reporting that the platforms are 'Safe to Operate' to the Operating and Delivery Duty Holders or other Accountable Persons, and are therefore responsible for leading the integration of System and Equipment-related safety information into the Platform Safety Case. The HLH managers shall ensure that hazards and risks associated with integration of the Systems and Equipments into the Platform are adequately captured and managed in the rationalised Hazard Log.

H.7.2. This integrated approach does not detract from the responsibilities of the relevant Platform, System or Equipment Authority to ensure the through life management of the safety regime, Safety Case information and Hazard Log information. Safety Authorities must work effectively to assess, manage and respond to changes which affect the hazards, risks and therefore the overall safety argument and Safety Case.

H.8. High Level Hazard Management Activities

H.8.1. Stages 1-6 of this leaflet remain the overarching guidance, therefore, management activities described here will only complement what has already been described. Notwithstanding, some tailoring is required at a lower level to ensure the rationalised Hazard Logs continue to deliver on their desired proportionality, thus the following additional guidance is provided against each stage of the process.

H8.2. Stage 1 – Hazard identification

H.8.2.1. It is to be expected that, in the majority of cases, any new safety risks that are identified can be incorporated into one of the existing HLHs. Should any hazards or risks be identified that do not align to the current SFM, changes to the SFM shall be proposed in accordance with the process at Annex H.

H.8.2.2. The newly identified risk must be structured to follow the bow-tie structure, and then compared to the existing causes and risks captured in the HLH. If neither the cause nor risk is already captured, it shall be incorporated into the HLH. It may be possible that the cause(s) and / or risk(s) is already captured, in which case the Hazard Log Co-ordinator shall ensure that the 'write once, use often' principle is applied and that duplication of information is avoided.

H.8.2.3. Any actions identified for the "new risk" shall be compared against the existing and current actions recorded in the rationalised Hazard Log to make sure that actions are not duplicated. For example, if the hazard can be mitigated through implementation of an ongoing A&A, the action that refers to this A&A shall be used instead of being duplicated, and the action record amended accordingly to reflect any new changes at this time.

H.8.2.4. Integration Of New Systems Or Equipments Into The Rationalised Hazard Logs

H.8.2.4.1. Where System or Equipment Authoritirs are conducting preliminary hazard identification for new Systems or Equipments, the relevant PA representatives shall attend to ensure:

H.8.2.4.1.1 Early capture of platform context;

H.8.2.4.2. Identification of risks for integration into the rationalised platform Hazard Log in accordance with the SFM and existing HLHs. This integration may take place once the EA has implemented appropriate controls; and

H.8.2.4.3. That the focus is on the risk to the end user on the platform.

H.8.2.4.2. As appropriate, the guidance on Safety Planning shall be followed to ensure effective planning and management of the system or equipment information captured in the Platform Safety Case and Hazard Log.

H.8.2.4.3. EAs delivering Equipment which is used independently of Platforms will continue to manage their own Safety Cases and Hazard Logs.

H.8.3. Stage 2 – Risk Analysis and Assessment

H.8.3.1. A key benefit of rationalisation is the ability to focus risk reduction effort on the risks with the highest frequency, worst severity or highest risk classification. Therefore as well as identifying the risk classification of each individual accident sequence, the Hazard Manager shall assess all the risks in the HLH to determine those which should be prioritised for risk reduction effort.

H.8.4. Stage 3 – Generating Options for Risk Control

H.8.4.1. All risks require control, and for the majority of risks on in-service platforms, those controls will already exist and be applied to other risks. Therefore it can be anticipated that for the newly identified cause or risk, many of the necessary control measures will already be captured in the rationalised Hazard Log.

H.8.4.2. In order to maintain the efficiency of the rationalised Hazard Logs, control measures are also to follow the 'write once, use often' principle. Once control measures for the cause / risk have been identified, the existing control measures shall be checked to ensure that duplicate records are not created.

H.8.4.3. HLH managers should note that whilst Naval Authority Certification is evidence of risk control for key hazard areas, the certification in itself is not fully comprehensive evidence of risk reduction or risk management; HLH managers should therefore be wary of complacency in consideration of other risk control measures.

H.8.5. Stage 4 – Implementing Risk Control Measures

H.8.5.1. Implementation of risk control measures does not vary from the core process and all actions shall be executed and pursued in accordance with the guidance in stages 1-6 of this Leaflet with a view to reducing the identified risks to the tolerable and ALARP level.

H.8.5.2.Actions

H.8.5.2.1. As each HLH will have a reasonable quantity of associated cause, risk and mitigation information attached to it, it is inevitable that there will be corresponding actions. These actions range from those that affect the hazard and risk in itself i.e. that may affect the risk classification, to those which are more routine such as administrative action to update a reference in the Hazard Log. In order to distinguish between these actions, the following definitions will be applied:

H.8.5.2.1.1 SIGINIFICANT ACTION – A Signification Action is considered to be:

H.8.5.2.1.1.1 Any action where the outcome could change the likelihood of any cause, frequency or subsequent risk classification;

H.8.5.2.1.1.2. Any action that warrants senior management attention.

H.8.5.2.1.1.3. **Note:** HLHs with significant actions should have an Accident descriptor of either OPEN, or MANAGED if they were ALARP prior to the action being raised.

H.8.5.2.1.2. ROUTINE ACTION – A Routine Action is an action of a routine nature that doesn't affect the risk classification or maturity status of the hazard concerned e.g. Update of BR reference etc.

H.8.5.2.1.2.1. **Note:** Any HLH may have a number of routine actions open against it and remain of ALARP.

H.8.5.2.2. Only significant actions shall be recorded in the rationalised Hazard Log, thus ensuring the focus remains on the risk to life issues. Routines actions shall be tracked and managed through the Hazard Review process.

H.8.5.2.3. As stated previously, captured actions shall follow the 'write once, use often' principle, and new actions shall be cross-checked with existing actions to ensure information is not duplicated in the Hazard Log tool.

H.8.5.3. Action Updates

H.8.5.3.1. For the purpose of expediting actions and maintaining the currency of the information in the Hazard Log, action updates shall be conducted as follows:

H.8.5.3.2. Significant actions – HLH managers can provide updates for open significant actions at any time, with the relevant information being entered by the HLC. This will help to ensure action information is up-to-date for hazard reviews. Significant actions can only be closed off after acceptance by the relevant SQEP panel, and appropriate minutes shall be referenced in the action record.

H.8.5.3.3. Routine actions – HLH managers can provide updates and close off open routine actions at any time, with the relevant information being entered by the HLC, unless the hazard manager assesses that the outcome of the routine action update / closure could convert the routine action to a significant action. For example, what appears to be a simple update to a BR reference becomes a significant action when it becomes apparent that the BR has had a major re-write and is now missing procedures that have been provided as mitigating evidence.

H.8.6. Stage 5 – Risk Acceptance

H.8.6.1 Risk acceptance for risks in rationalised Hazard Logs shall follow the process described in the main body of this Leaflet.

H.8.6.2. However, when undertaking risk acceptance, the HLH manager shall assess where the new risk lies in relation to the existing risks in terms of classification and maturity status, and if necessary re-prioritise the associated risks and actions in order to focus risk reduction effort as follows:

H.8.6.2.1. OPEN Risks;

H.7.6.2.2. MANAGED Risks;

H.8.6.2.3. Where risk are ALARP, then risks with the highest risk classification. Where there are large numbers of risks with the same classification, they shall be prioritised according to accident severity.

H.8.6.3. Once the risk assessment has been completed, the Hazard Manager shall submit all changes to the HLH to the HLC for capture in the rationalised Hazard Log.

H.8.7. Stage 6 – Risk Review

H.8.7.1. HLH risks shall be reviewed in accordance with stage 5 of this Leaflet. However, there may be other points at which HLH managers may wish to revisit the HLH information to understand if changes are required, such as:

H.8.7.1.1. Update to or completion of open significant actions against the hazard;

H.8.7.1.2. Development and implementation of Design Changes (A&As, Class Modifications);

H.8.7.1.3. Preparation and outcome of Minor/Fleet Trials and Test data;

H.8.7.1.4. In Service Reporting for significant events – Signals/S2022s etc.;

H.8.7.1.5. Fitting of Military Task Equipment (MTE);

H.8.7.1.6. Concession requests;

H.8.7.1.7. Generation of System / Equipment Safety Cases;

H.8.7.1.8. Key Hazard Area submissions to Naval Authorities;

H.8.7.1.9. Incidents or accidents in ships whose circumstances are reported to DE&S staff;

H.8.7.1.10. Incidents or accidents report via Navy Lessons and Incident Management System (NLIMS);

H.8.7.1.11. Product Alert Notice;

H.8.7.1.12. Removal or recantation of an existing control measure;

H.8.7.1.13. Feedback from a Platform Safety and Environmental Committee.

H.8.7.2. Where individual risks associated with the overarching HLH are adequately reduced to a tolerable and ALARP position, the remainder of the risks captured in the HLH shall be reviewed from Stages 2-5 to identify those now requiring the most risk reduction effort.

H.9. Reporting

H.9.1. Reporting for the rationalised Hazard Logs shall take place in accordance with POSMS (SMP11) and for the following occasions as a minimum:

H.9.1.1. Platform Safety and Environmental Committees;

H.9.1.2. Relevant Safety and Environmental Case Report updates;

H.9.1.3. Safety Argument updates;

H.9.1.4. Command Safety and Environmental Summary updates;

H.9.1.5. As required for assurance and audit purposes.

H.9.2. Whilst the Hazard Log tool in use will be capable of generating reports on hazards and risks in terms of number, risk classification and Accident status, it is recommended that the platform teams using the rationalised Hazard Logs use the Safety Function Model Report to illustrate the risks which have been prioritised for risk reduction effort. In addition, this report can be used to display the highest risk status of the risks against the HLH, and provides quick reference data to determine if any risks have an Accident status that is not ALARP or at least MANAGED.

H.9.3. This report would be maintained by the Platform Safety Managers on the basis of the information communicated by the HLH Managers.

H.9.4. In order to provide this report, Safety Managers shall:

H.9.4.1. Ensure the Safety Function Model Report is appropriately tailored to include the applicable functions for the platform in question;

H.9.4.2. Maintain an up-to-date version of the report for amendment only by the HLC / safety team;

H.9.4.3. Ensure the HLHs in the Hazard Log reflect the correct Safety Function area from the SFM;

H.9.4.4. Ensure the HLH risks with the highest probability, frequency and overall risk – as determined by the hazard manager – are correctly captured in the report;

H.9.4.5. Ensure the overall Accident status for the HLH is correctly captured in the report;

H.9.4.6. Add any supporting comments to the HLH as required e.g. where risk assessments are required, or to justify an Accident status of OPEN.

APPENDIX 1 TO ANNEX H – SAFETY FUNCTION MODEL

Top Level Function		Top Level Function Scope	2nd Level Function		2nd Level Function Scope	3rd Level Function	3rd Level Function Scope	ANEP 77 Mapping
Function Number	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number**	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number and Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**The relevant Chapter of the Naval Ship Code which apples to this function**
1	Provide a safe platform	The ability to provide the basic habitability functions for personnel to work and live onboard the ship. Failure of these functions may not directly lead to risk to life but could a) start an accident sequence which affects other Safety Functions or b) remove a control measure which mitigates risk to life.						
			1.1	Maintain stability	The ability to maintain the stability of the platform			CHAPTER III - BUOYANCY, STABILITY AND CONTROLLABILITY
			1.2	Maintain structural Integrity	The ability to maintain the structural integrity of the ship, inclusive of hull, superstructure and internal boundaries			CHAPTER II – STRUCTURE
						1.2.1 Maintain hull integrity	Maintenance of the ships hull and superstructure integrity	IV-13
						1.2.2 Maintain bulkhead integrity	Maintenance of the superstructure, and internal boundaries	IV-2
						1.2.3 Maintain load / lifting points	Maintenance of lifting / load points, but not their use.	X-2
								III-4
			1.3	Provide power	The ability to provide power for the systems and equipments on the ship - inclusive of electrical, hydraulic and pneumatic power. This includes the ability to control provision of power through integrated systems			IV-4
			1.4	Provide cooling	The ability to provide heating / cooling inside the vessel			IV-23
			1.5	Provide lighting	The ability to provide lighting on the vessel, both internally and for the upper deck / flight deck			IV-11
			1.6	Provide Ventilation/ Circulatory Air	The ability to provide and circulate breathing air throughout the vessel			IV-20

Top Level Function		Top Level Function Scope	2nd Level Function		2nd Level Function Scope	3rd Level Function	3rd Level Function Scope	ANEP 77 Mapping
Function Number	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number**	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number and Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**The relevant Chapter of the Naval Ship Code which apples to this function**
			1.7	Manage access	The ability to provide safe access and transit throughout the ship. This function includes transit of ladders, but does not include working at height			II-3
			1.8	Provide Communication	The ability to provide communications both internal and external to the ship.			CHAPTER VIII - COMMUNICATIONS
						1.7.1. Provide internal communications	The ability to communicate within the ship.	VIII: -6 Internal Communication VIII-7 Main broadcast
								VIII–8 Portable Communication
						1.7.2 Provide external communications	The ability to transmit and receive communications from outside the ship.	VII-13
								VII-
2	Control ship movement	The ability to maintain the safety of the ship whilst it is carrying out its tasking						CHAPTER IX - NAVIGATION
			2.1	Maintain situational awareness	The ability to know and understand the environment the ship is in - both for navigation and capability purposes			
						2.1.1 Knowledge of navigational hazards	The ability to detect navigational hazards	IX-6
						2.1.2 Maintain tactical picture	The ability to understand the tactical situation through provision of tactical data	IX-11
			2.2	Control speed	The ability to control the speed of the vessel			
						2.2.1 Provide propulsion	Provision of propulsion	Part1-IV-5
								Part1-IV-13
			2.3	Control direction	The ability to control the direction of the vessel			
						2.3.1 Provide steering	Provision of steering	IV-5
3	Control weapons and Ordnance, Munitions and Explosives (OME)	The ability to control ordnance, munitions and explosives onboard the vessel, including spent weapons or munitions. This scope covers any materials governed by JSP 862 Naval						CHAPTER X - DANGEROUS GOODS

Top Level Function		Top Level Function Scope	2nd Level Function		2nd Level Function Scope	3rd Level Function	3rd Level Function Scope	ANEP 77 Mapping
Function Number	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number**	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number and Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**The relevant Chapter of the Naval Ship Code which apples to this function**
		Magazine and Explosives Regulations	3.1	Safe handling of weapons and OME	The ability to safely handle weapons and munitions onboard - this covers movement of munitions and spent weapons during embarkation / disembarkation, and movement between magazines / stores and weapons / launchers			X-10
			3.2	Safe storage of weapons and OME	The ability to safely store weapons and munitions onboard, including spent weapons where necessary			X-10
			3.3	Control dynamic safety of weapons and OME	The ability to safely use weapons and munitions onboard, including the ability to safely recover spent weapons where necessary			X-10
4	Control seamanship evolutions	The ability to control hazardous seamanship evolutions which need to be undertaken by all RN ships at sea						
			4.1	Dock / ballasting operations	The ability to conduct ballasting / docking operations safely, for ships which provide this function for additional craft i.e. LPD / LPH / LSD(A)			II-5
			4.2	Boat / landing craft operations	The ability to safely carry out boat / landing craft launch and recover procedures. This does not include boat transfers			VII-22
								IX-7
			4.3	Control Replenishment at Sea (RAS) operations	The ability to safely conduct Replenishment at Sea			IV-19
								IX-7
			4.4	Control berthing / anchoring / towing	The ability to safely conduct high risk seamanship evolutions			IV-20
								IX-6
			4.5	Control personnel embarkation / disembarkation	The ability to safely conduct boat transfers between the ship and another vessel. This includes transfer of luggage and small goods			IX-13
5	Control fire and damage	The ability to control situations which are hazardous to personnel onboard						CHAPTER VI - FIRE SAFETY
			5.1	Fire prevention	The ability to prevent fire			VI-3
			5.2	Fire detection	The ability to detect fire			VI-7
			5.3	Fire suppression	The ability to fight fire			VI-9

Top Level Function		Top Level Function Scope	2nd Level Function		2nd Level Function Scope	3rd Level Function	3rd Level Function Scope	ANEP 77 Mapping
Function Number	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number**	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number and Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**The relevant Chapter of the Naval Ship Code which apples to this function**
								VI-8
								VI-6
			5.4	Action damage control	The ability to recover from action damage			VI-8
								IV-9
								X-11
								II-2
								VI-2
								VI-5
			5.5	Flood control	The ability to prevent, detect and fight floods. NB there may be some overlap with functions 1.1 / 1.2 when considering floods, care should be taken to consider the accident sequence described to choose which hazard the accident sequence is captured in			II-2
								II-3
								III-3
								III-4
								IV-10
			5.6	Exposure to chemical, Biological, Radiological and Nuclear (CBRN) Agents	The ability to detect and remove / minimise the risks of CBRN warfare hazards to the individual			
6	Enable escape and evacuation	The ability to both evacuate compartments within the ship, as well as to abandon ship if required						X
			6.1	Evacuation	The ability to evacuate compartments within the ship .e.g for fire			VII – All Regulations
			6.2	Escape and survival	The ability to escape the vessel if required .e.g abandon ship			VII- 24,25,26,27
7	Control specific equipment hazards	The ability to control hazards linked to use of specific platform equipment and systems						CHAPTER IV - ENGINEERING SYSTEMS
			7.1	Moving machinery	Risks to personnel from proximity to moving machinery.			IV-18
								VII15

Top Level Function		Top Level Function Scope	2nd Level Function		2nd Level Function Scope	3rd Level Function	3rd Level Function Scope	ANEP 77 Mapping
Function Number	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number**	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number and Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**The relevant Chapter of the Naval Ship Code which apples to this function**
			7.2	Lifts / Lifting activities	The risk to personnel from lifts and lift machinery e.g. food lifts / weapons lifts / personnel lists. Not to be confused with lifting activities such as slinging or use of cranes and davits.			IV-22
								VI-8
			7.3	Lifting and Slinging	The risk to life from slinging activities through use of cranes / davits / lifting eyes etc.			IV-22
								VI-8
			7.4	Black/Grey water systems	Risk to life from use of black and grey water systems. This includes transfer of waste to other vessels / vehicles			Not in ANEP 77
								IV-4
								IV-24
			7.5	Pressurised Systems	Risk to life from use of pressurised systems. This includes hydraulic and pneumatic systems, and also covers portable pressurised systems.			IV-6
			7.6	Unmanned vehicles	Risk to life from use of unmanned vehicles. This covers air, surface and sub-surface capability.			VI-8
								X-10
								IV-25
8	Control aviation hazards	The ability to safely operate aircraft from the ship						Chapter VII
			8.1	Secure aircraft	The ability to secure aircraft both on the flight deck and in the hangar			VI-13
			8.2	Maintain aircraft	The ability to maintain aircraft on the ship			IV-8
								IV-11
								IV-23
			8.3	Move aircraft	The ability to move aircraft on the deck i.e. between the hangar and the flight deck			IV-22
			8.4	Launch / recover aircraft	The ability to safely launch and recover the aircraft from the ship. Includes VERTREP procedures			II-3
								IX-7
								X-10
			8.5	Respond to aircraft emergencies	The ability to respond to aircraft emergencies. This includes emergencies where the aircraft does not return to the ship			X-10
								X-11

Top Level Function		Top Level Function Scope	2nd Level Function		2nd Level Function Scope	3rd Level Function	3rd Level Function Scope	ANEP 77 Mapping
Function Number	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number**	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number and Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**The relevant Chapter of the Naval Ship Code which apples to this function**
			8.6	Provide safe airspace	The ability to provide safe airspace to the ships aircraft, and to any aircraft operating with the ship			X-10
9	Control radiated energy	The ability to control all ionising and non-ionising radiation sources / signatures onboard the vessel. This function also covers the ability of the ship to protect its personnel from sources on adjacent platforms (ships / aircraft)						
			9.1	Control laser emissions	The ability to control laser emissions.			IX-11
								IV-17
								IV-18
			9.2	Control radar emissions	The ability to control radar emissions			IX-11
								IV-17
								IV-18
			9.3	Control wireless telegraphy	The ability to control radio emissions across the spectrum			IV-17
								IV-18
			9.4	Control sonar emissions	The ability to control sonar emissions			IV-17
								IV-18
			9.5	Control magnetic signature	The ability to control the magnetic signature of the ship.			
10	Control hazards to the individual	The ability to control general hazards which cannot be avoided in the execution of duties on a ship						
			10.1	Control hazardous materials	The ability to control hazardous materials. These are materials that are deliberately carried onboard to support a specific function. This does not cover substances which are created inadvertently			II-7
								II-8
								VI-5
			10.2	Prevent / respond to man overboard	The ability to prevent or respond to man overboard situations			VII-27
								III-6
			10.3	Prevent electric shock	The ability to prevent both electric shock and electrocution			Part1-IV-10
								Part1-IV-12
			10.4	Provide safe food / drinking water				IV-24

Top Level Function		Top Level Function Scope	2nd Level Function		2nd Level Function Scope	3rd Level Function	3rd Level Function Scope	ANEP 77 Mapping
Function Number	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number**	**Function Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**Function Number and Name**	**Description of what this function covers and, where relevant, what it does not cover.**	**The relevant Chapter of the Naval Ship Code which apples to this function**
					The ability to provide safe food and drinking water for embarked personnel			Habitability Part 3 1B-9
			10.5	Control exposure to noise / vibration	The ability to control exposure to noise or vibration.			Part1-IV-17
								Part 1-IV-18
								X-3
								IV-18
			10.6	Prevent Exposure to biological and bacterial agents	The ability to control exposure to agents which are not supposed to be onboard but which may occur inadvertently e.g. legionella. This does not include biological warfare agents (see function 5.6)			Not specifically addressed in ANEP but see Naval Ship Characteristic Habitability on Page Part 3 1B-9
			10.7	Manual Handling	The ability to control the risk of manual handling injuries			Not specifically addressed in ANEP but see Naval Ship Characteristic Habitability on Page Part 3 1B-9

11	Control safe conduct of work	The ability to control the way hazardous activities are undertaken to minimise risk to life. This function covers any work to be undertaken onboard the vessel whilst the 'Safe to Operate' responsibility is discharged by the Platform Authority. Therefore this function covers work undertaken by Ships Staff;' Class Output Management (COM) staff; Service Providers; Original Equipment Manufacturers; and any other agency / organisation as required by the Platform Team.						
			11.1	Provide safe systems of Work	Provision of processes and procedures which specify safe ways to conduct activities			X-10
						11.1.1 Control diving operations	The ability to safely conduct diving operations	X-10
						11.1.2 Control working at height	The ability to safely conduct working at height	IX-7
						11.1.3 Control access to confined spaces	The ability to safely access and work in confined spaces. A confined space as defined by the HSE is a place which is substantially enclosed (though not always entirely), and where serious injury can occur from hazardous substances or conditions within the space or nearby (e.g. lack of oxygen).	IV-18
						11.1.4 Control high risk maintenance	The ability to control high risk maintenance	VII-2
								X-11
			11.2	Provide Safe Processes	The ability to ensure the processes and procedures provided are fit for purpose	11.2.1 Standard & Emergency Operating procedures		X-11
						11.2.2. Operating Instructions		
						11.2.3 Maintenance Cards		

APPENDIX 2 TO ANNEX H – CHANGES TO THE SAFETY FUNCTION MODEL

H.10. Proposing Changes to the Safety Function Model

H.10.1. The SFM is a Ships OC-wide tool in support of this end-to-end management of risk process and therefore needs to cover all applicable platforms. It is recognised that as project teams transfer existing Hazard Logs to rationalised Hazard Logs, additional Safety Functions may be identified for capture in the model; change in this area falls outside the tailoring detailed above, and changes to the model will need OC-wide acceptance prior to incorporation.

H.10.2. Users should demonstrate adequate caution in identifying new Safety Functions, as any change to the SFM may have a corresponding ripple effect on other teams and could cause un-necessary rework.

H.10.3. The following process for change to the SFM should be applied:

H.10.3.1. Step 1 – the required change should be identified within the project team and communicated to the Leaflet 5 owner, with a recommendation for where it should be incorporated into the model;

H.10.3.2. Step 2 – the leaflet 5 owner will check the SFM to ensure it is not already captured. If it is not, the leaflet 5 owner will communicate initial approval back to the proposer;

H.10.3.3. Step 3 – the proposer should submit the proposed changes to the other team Chief Engineers. This will allow the other platform teams an opportunity to assess how the change affects their platform and whether it introduces any unnecessary re-work on their part;

H.10.3.4. Step 4- Platform Chief Engineers consider their proposal and approve or otherwise. The decision should be communicated back to the proposer.

H.10.3.5. Step 5 – the Proposer should collate the responses and present to the leaflet 5 owner for consideration and decision.

H.10.3.6. Step 6 – the leaflet 5 owner incorporates the proposed change or otherwise as follows;

H.10.3.6.1. Full consensus from all Chief Engineers – change incorporated into the Safety Function Model;

H.10.3.6.2. Partial consensus from Chief Engineers – leaflet 5 owner considers the dissenting arguments and makes a final decision about incorporation.

H.10.4. The SFM Change Process is illustrated in the swimlane diagram at figure H-1.

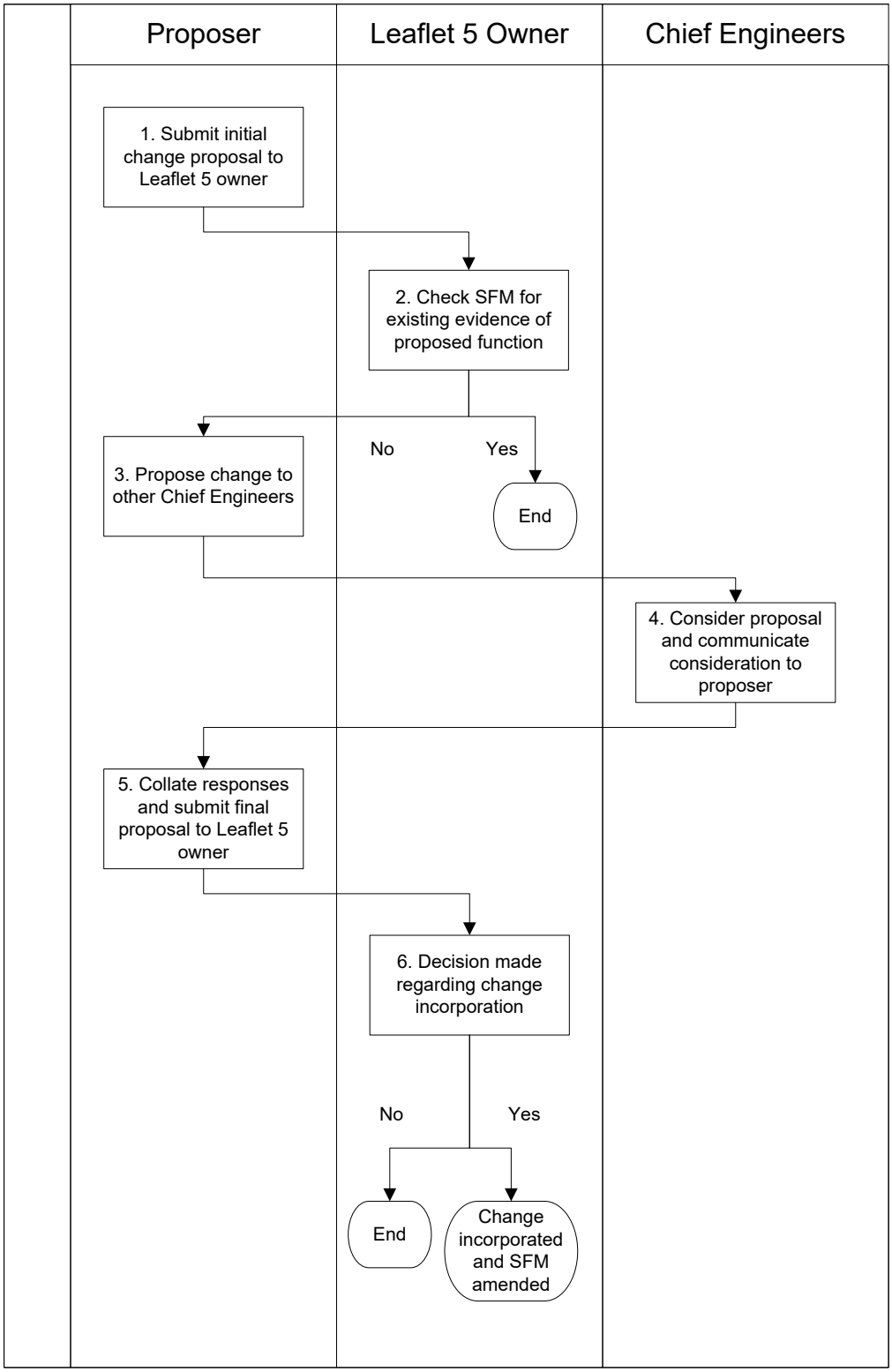


Figure H-1 - Swimlane Diagram for Safety Function Model Changes

ANNEX I – RISK ACCEPTANCE TEMPLATES

I.1. In accordance with the Risk Acceptance Process and Guidance at Section 10 of this Leaflet, the Risk Summary Template and Declaration Statements below are designed to be used to provide a clear audit trail to demonstrate that Risks have been suitably agreed, endorsed and ultimately accepted by the relevant Duty Holders[21] or other Accountable Persons[22].

Risk Summary Template

Unique ID:						
Equipment:						
System:						
Platform(s):						
Hazard Description:						
Risk Assessment[23]:	**Accident Frequency:**		**Consequence Definition:**		**Risk Classification:**	
Description of Accident Consequences:						

Risk Control Measures Implemented	
Risk Control Measure	**DLOD Owner**

Risk Reduction Measures Considered but not Implemented	
Potential Risk Control Measure	**Justification for Non Implementation**

Outstanding Actions required to remain ALARP		
Action	**Owner**	**Target Date**

Accident Status:	
ALARP Statement:	

[21] As defined in 1SL/CNS/1/2 dated 21 Mar 17 – Duty Holding in the Royal Navy.

[22] In this context, Accountable Persons may be individuals within the Chain of Command who are not Duty Holders but have direct responsibility for activities that generate Risk, or individuals within DE&S Platform/Equipments Authorities who are formally authorised to accept Risks on behalf of a Duty Holder or other Accountable Person. In all instances, Risk ownership and thus ultimate accountability rests with the Front Line Command.

[23] In accordance with the Common Risk Classification Matrix at Annex D to this Leaflet.

Hazard Manager Declaration Statement

- As the formally appointed Hazard Manager, I hereby declare that the information above is an accurate summary of the Risk in question. Additional details are captured in the *[Insert Name of Equipment/System/Platform]* Hazard Log and can be made available on request.
- The above information has been agreed by a SQEP Panel in which all relevant stakeholders were represented by suitably empowered SQEP individuals. Details of those in attendance are retained within Project records and can be made available on request.

Hazard Manager:	**Name:**		**Assignment:**		**Contact Number:**	
	Signature:				**Date:**	

ISA Declaration Statement (where appropriate)

- As the formally appointed Independent Safety Auditor (ISA) for *[Insert Name of Equipment/System/Platform]*, I hereby endorse that, subject to the coments below, the information above is an accurate summary of the Risk in question and meets the requirements of relevant policy, procedures and recognised good practice.

ISA Comments						
ISA:	**Name:**		**Assignment:**		**Contact Number:**	
	Signature:				**Date:**	

PSEC Chairman's Declaration Statement

- As the formally appointed Chairman of the *[Insert Name of Equipment/System/Platform]* Safety and Environmental Committee, I hereby declare that the information above is an accurate summary of the Risk in question. Additional detail is captured in the relevant Hazard Log and can be made available on request.
- The above information has been agreed by a SQEP Panel, endorsed by an Independent Safety Auditor (ISA) and subsequently authorised by the *[Insert Equipment/System/Platform]* Safety and Environmental Committee in which all relevant stakeholders were represented by suitably empowered SQEP individuals. Details of those in attendance at the SQEP Panel and the Safety and Environmental Committee are retained within Project records and can be made available on request.

PSEC Chairman:	**Name:**		**Assignment:**		**Contact Number:**	
	Signature:				**Date:**	

Duty Holder/Accountable Person Declaration Statement

- As the formally appointed Senior/Operating/Delivery (delete as appropriate) Duty Holder or other suitably empowered Accountable Person, I hereby confirm acceptance of the Risk summarised above.

Duty Holder or Accountable Person:	**Name:**		**Assignment:**		**Contact Number:**	
	Signature:				**Date:**	