HAZARD IDENTIFICATION AND RISK ASSESSMENT PROCEDURE

Hazard Identification and Risk Assessment

Document Title	Hazard Identification and Risk Assessment Procedure
Document Ref	SM/HSE/PRO/001
ISO Standard	ISO 45001:2018
ISO Clauses	6.1.1, 6.1.2, 6.1.3, 6.1.4
Version	1.0
Classification	Internal
Effective Date	15 March 2026
Review Date	15 March 2027
Approved By	Darren Watts, Group Compliance Director
Supersedes	New document – no prior version

1. PURPOSE

This procedure establishes the systematic process for identifying workplace hazards, assessing occupational health and safety (OH&S) risks, and determining appropriate controls across all Seagull Maritime Group operations. It ensures that OH&S risks are identified, evaluated, and managed before work activities commence and throughout their duration.

This procedure directly supports the commitments made in the OH&S Policy (SM/HSE/POL/001) and provides the operational framework for meeting ISO 45001:2018 Clause 6.1 requirements for planning actions to address risks and opportunities.

2. SCOPE

This procedure applies to all occupational health and safety hazards and risks across the Seagull Maritime Group, including:

- Shore-based offices (Dubai, Greece, UK, Nigeria)
- Vessel-based operations (Security Escort Vessels, client vessels, transfer operations)
- Field operations across all regions (Indian Ocean Region, West Africa, Persian Gulf)
- Seagull Offshore operations (fisheries protection, vessel provision services)
- All personnel: shore-side staff, Private Contracted Armed Security Personnel (PCASP), vessel crew, contractors, and visitors

This procedure covers OH&S risks only – those relating to injury, ill-health, and occupational safety. Security threats, geopolitical risks, and business risks are assessed under a separate procedure (SM/SEC/PRO/001 – Security and Business Risk Assessment Procedure) using the RA-004 methodology. Where an activity presents both OH&S and security risks, both procedures apply and both assessments shall be completed.

3. REFERENCES

- ISO 45001:2018 – Occupational Health and Safety Management Systems (Clauses 6.1.1, 6.1.2, 6.1.3, 6.1.4)
- SM/HSE/POL/001 – OH&S Policy
- SM/HSE/DOC/001 – OH&S Management System Scope Statement
- SM/INT/DOC/002 – Context of the Organisation
- SM/HSE/RA-003 series – OH&S Risk Assessment Template (5×5 matrix)
- SM/SEC/PRO/001 – Security and Business Risk Assessment Procedure (cross-reference)
- SM/INT/PRO/001 – Non-Conformance, OFI and Corrective Action Management
- BMP-MS (Best Management Practices – Maritime Security) – for maritime-specific hazard context
- MISTO (Maritime Information Sharing and Threat Overview) – for threat environment context

4. DEFINITIONS

Hazard: A source or situation with the potential to cause injury or ill-health.

Risk: The combination of the likelihood of a hazardous event occurring and the severity of injury or ill-health that the event could cause.

Risk Assessment: A systematic process of identifying hazards, evaluating the associated risks, and determining appropriate controls to eliminate or reduce the risk to an acceptable level.

Residual Risk: The level of risk remaining after controls have been applied.

ALARP (As Low As Reasonably Practicable): The principle that risk should be reduced to the lowest level that is reasonably practicable, balancing the cost and effort of further reduction against the benefit gained.

Competent Person: A person with the necessary training, experience, and knowledge to conduct or review a risk assessment for the activity in question.

Hierarchy of Controls: The systematic approach to eliminating or reducing risk, prioritised from most to least effective: elimination, substitution, engineering controls, administrative controls, personal protective equipment (PPE).

Near Miss: An unplanned event that did not result in injury or ill-health but had the potential to do so.

Inherent Risk: The level of risk present before any controls are applied.

5. ROLES AND RESPONSIBILITIES

5.1 Group Compliance Director

- Owns this procedure and the OH&S risk assessment methodology
- Reviews and approves all completed risk assessments before they are issued
- Maintains oversight of the risk assessment programme and schedule
- Escalates critical risks to the CEO and senior management
- Ensures risk assessments are updated following incidents, near misses, or changes in the operating environment
- Completes default controls on standard operational risk assessments (RA-003 series)

5.2 QHSE Manager (When Appointed)

- Manages the day-to-day scheduling and tracking of risk assessments
- Quality-checks completed risk assessments for methodology compliance
- Coordinates with operations managers to ensure assessments are current
- Reports risk assessment status to the Group Compliance Director

5.3 Operations Managers and Project Team Leads

- Conduct risk assessments for their areas of responsibility using the RA-003 template
- For standard operational risk assessments: review default controls, report any changes or additions required to reflect actual conditions
- For new or project-specific risk assessments: complete all control fields to demonstrate hazard management before task approval
- Ensure all personnel under their supervision are briefed on relevant risk assessments and controls
- Report new or changed hazards to the Group Compliance Director or QHSE Manager

5.4 All Workers

- Participate in hazard identification and risk assessment activities when required (ISO 45001, Clause 5.4)
- Report hazards, near misses, and unsafe conditions through the Emergent HSE App or direct reporting to their supervisor
- Follow the controls identified in relevant risk assessments
- Do not undertake any task where they believe the risk has not been adequately assessed or controlled

6. HAZARD IDENTIFICATION

Hazard identification is a proactive, ongoing process. It does not occur only when a formal risk assessment is scheduled. All personnel are responsible for identifying and reporting hazards as part of their normal duties.

6.1 Sources of Hazard Information

The following sources shall be used to identify OH&S hazards across all operations:

6.1.1 Internal Sources

- Incident and near-miss reports from the Emergent HSE App
- Internal audit findings and non-conformance reports (SM/INT/PRO/001)
- Worker feedback, toolbox talks, and safety briefings
- Equipment inspection and maintenance records
- Training records and competence assessments
- Operational task data from 1Clearview ERP (personnel deployments, vessel assignments, equipment status)
- Previous risk assessments and their review outcomes
- Management review outputs

6.1.2 External Sources

- UKMTO advisories and JMIC maritime security assessments
- MSCHOA (Maritime Security Centre – Horn of Africa) updates
- IMB Piracy Reporting Centre reports
- BMP-MS and MISTO guidance for maritime-specific hazards
- Client-specific requirements and intelligence briefings
- Flag state and port state requirements
- Industry body guidance (e.g., SAMI legacy publications, ICoCA, IMO circulars)
- Conflict zone monitoring (daily operational intelligence on Persian Gulf, Red Sea, Gulf of Aden, GCC region)
- War risk insurance and P&I Club advisories

6.2 Categories of Hazard

Hazard identification shall consider, as a minimum, the following categories:

- Routine activities: tasks performed regularly as part of normal operations (vessel embarkation/disembarkation, bridge watches, equipment cleaning)
- Non-routine activities: tasks performed infrequently or in response to unusual circumstances (emergency drills, unscheduled maintenance, new vessel familiarisation)

- Emergency situations: fire, man overboard, vessel collision, medical emergency, piracy attack, armed confrontation
- Human factors: fatigue from shift patterns and extended deployments, lone working, communication barriers (multilingual crews), stress, substance misuse
- Workplace design and conditions: vessel deck layout, accommodation standards, lighting, ventilation, noise, temperature extremes, sea state
- Environmental hazards: extreme weather, high sea states, tropical diseases, heat stress, UV exposure
- Equipment and materials: weapons handling and storage, ammunition, pyrotechnics, communications equipment, vessel machinery
- Changes: new operations, new routes or regions, changes to vessel or equipment, regulatory changes, changes in threat environment
- Contractors and visitors: personnel not familiar with vessel or site-specific hazards

7. RISK ASSESSMENT METHODOLOGY

All OH&S risk assessments shall use the RA-003 (5×5) risk matrix. This methodology assesses risk as the product of likelihood and severity, producing a risk score between 1 and 25.

7.1 Likelihood Scale

Likelihood is assessed on a scale of 1 to 5 based on the probability of the hazardous event occurring, considering current conditions and available intelligence:

Rating	Likelihood	Description
1	**Rare**	Could occur only in exceptional circumstances. No history of occurrence within the company or similar operations.
2	**Unlikely**	Could occur but not expected. Has occurred in the wider maritime security industry but not within Seagull Maritime operations.
3	**Possible**	Could occur at some time. Has occurred previously within similar operations or there are known near misses.
4	**Likely**	Will probably occur in most circumstances. Has occurred within Seagull Maritime operations or similar companies in the last 12 months.
5	**Almost Certain**	Expected to occur in most circumstances. Has occurred repeatedly or conditions make occurrence highly probable.

7.2 Severity Scale

Severity is assessed on a scale of 1 to 5 based on the worst credible outcome of the hazardous event, focused on injury and ill-health to persons:

Rating	Severity	Description
1	Negligible	No injury or very minor injury requiring no more than basic first aid. No lost time. No medical treatment required.
2	Minor	Minor injury requiring medical treatment but no hospitalisation. Up to 3 days lost time. Minor ill-health effects that are fully reversible.
3	Moderate	Injury requiring hospitalisation or extended medical treatment. Between 3 and 14 days lost time. Reversible health effects requiring ongoing monitoring.
4	Major	Serious injury causing long-term disability or permanent impairment. More than 14 days lost time. Irreversible health effects. Single fatality.
5	Catastrophic	Multiple fatalities or injuries with life-changing consequences to multiple persons. Mass casualty event.

7.3 Risk Matrix

The risk score is calculated by multiplying the likelihood rating by the severity rating. The resulting score determines the risk classification:

Likelihood / Severity	1 - Negligible	2 - Minor	3 - Moderate	4 - Major	5 - Catastrophic
5 - Almost Certain	5	10	15	20	25
4 - Likely	4	8	12	16	20
3 - Possible	3	6	9	12	15
2 - Unlikely	2	4	6	8	10
1 - Rare	1	2	3	4	5

7.4 Risk Rating and Required Action

Risk Score	Rating	Required Action
1 – 4	Low	Acceptable risk. Monitor and review during scheduled assessments. No additional controls required unless reasonably practicable.
5 – 9	Moderate	Tolerable risk with monitoring. Review controls within 30 days. Consider additional measures to reduce risk further. Management awareness required.
10 – 16	High	Unacceptable without additional controls. Operations may proceed only with enhanced controls in place and documented approval from a competent person. Review within 7 days.
17 – 25	Critical	Unacceptable. Operations must not proceed until risk is reduced. Immediate escalation to the Group Compliance Director required. Senior management decision to proceed or suspend.

7.5 Inherent and Residual Risk

Every risk assessment shall record two risk scores for each identified hazard:

Inherent Risk (Pre-Controls): The risk level assessed before any controls are applied. This represents the raw exposure.

Residual Risk (Post-Controls): The risk level assessed after all identified controls have been applied. This represents the managed exposure and must demonstrate a meaningful reduction from the inherent score.

If the residual risk remains High or Critical after controls are applied, additional controls must be identified, or the activity must be escalated to the Group Compliance Director for a decision on whether to proceed, modify, or suspend operations.

7.6 ALARP Principle

All residual risks shall be reduced to a level that is as low as reasonably practicable (ALARP). A risk is ALARP when the cost, time, and effort required to reduce the risk further is grossly disproportionate to the benefit gained. The burden of proof lies with the person asserting that further risk reduction is not reasonably practicable.

8. HIERARCHY OF CONTROLS

Controls shall be selected and applied in order of effectiveness, following the hierarchy of controls required by ISO 45001:2018 Clause 8.1.2:

Priority	Control Type	Description	Maritime Example
1	**Elimination**	Remove the hazard entirely so it no longer exists.	Cancel a vessel transfer in sea state exceeding safe limits.
2	**Substitution**	Replace the hazard with something less dangerous.	Use a gangway system instead of a pilot ladder where feasible.
3	**Engineering Controls**	Isolate people from the hazard through physical means.	Install guard rails, non-slip deck surfaces, weapon storage lockers.
4	**Administrative Controls**	Change the way people work through procedures, training, signage, or scheduling.	Briefings before embarkation, rotation schedules to manage fatigue, toolbox talks.
5	**PPE**	Provide personal protective equipment as a last line of defence.	Body armour, life jackets, hard hats, safety boots, hearing protection.

Controls shall be applied in priority order. Lower-priority controls (PPE) are acceptable only when higher-priority controls are not reasonably practicable. Risk assessments must document why higher-priority controls were not applied where this is the case.

8.1 Control Completion – Standard vs. Project-Specific Assessments

Standard operational risk assessments (RA-003 series): The Group Compliance Director completes default controls reflecting established safe systems of work. Operations managers and project team leads shall review these defaults and report any changes, additions, or site-specific

adjustments required to reflect actual conditions. Changes are recorded in the risk assessment and approved before the assessment is reissued.

New or project-specific risk assessments: Control fields are left blank. The project team or operations manager conducting the assessment must complete all control fields before the task is approved. This provides evidence that the team has actively considered and addressed the hazards specific to their operation. The completed assessment is submitted to the Group Compliance Director (or QHSE Manager when appointed) for review and approval before work commences.

9. WHEN TO CONDUCT RISK ASSESSMENTS

Risk assessments shall be conducted or reviewed in the following circumstances:

9.1 Mandatory Triggers

- Before the commencement of any new operation, route, region, or tasking
- Before the introduction of new equipment, vessels, or working methods
- Following any incident, near miss, or reported unsafe condition
- Following a non-conformance or corrective action that identifies an uncontrolled or inadequately controlled hazard
- When there is a significant change to the operating environment (including conflict zone escalation, new threats, regulatory changes, or changes in war risk status)
- When a client imposes specific risk assessment requirements as part of their due diligence or operational instructions
- Following changes to personnel that affect competence levels (e.g., new PCASP with different training backgrounds)

9.2 Scheduled Reviews

- All risk assessments shall be reviewed at the frequency specified in the Document Register (SM/INT/REG/001). Review frequency is determined based on the nature and volatility of the hazards assessed.
- High-volatility assessments (e.g., region-specific operational risk assessments in active conflict zones) shall be reviewed at least quarterly or following any significant change in threat intelligence.
- Stable assessments (e.g., office-based risk assessments) shall be reviewed at least annually.
- All risk assessments shall be reviewed as part of the annual management review cycle.

10. RISK ASSESSMENT PROCESS

The following step-by-step process shall be followed for all OH&S risk assessments:

Step 1: Define Scope and Activity

Clearly define the activity, operation, or workplace being assessed. Record the location, personnel involved, equipment in use, and any relevant environmental conditions or constraints.

Step 2: Identify Hazards

Using the sources and categories in Section 6, systematically identify all hazards associated with the activity. Consider routine, non-routine, and emergency scenarios. Consult workers who perform the activity (Clause 5.4 requirement).

Step 3: Identify Who Is at Risk

For each hazard, identify who could be harmed and how. Consider all categories of personnel: PCASP, vessel crew, shore-based staff, contractors, clients, visitors, and members of the public where applicable.

Step 4: Assess Inherent Risk

Using the likelihood and severity scales in Section 7, assess the inherent risk score for each hazard — that is, the risk level before any controls are applied. Record the likelihood, severity, and resulting risk score in the RA-003 template.

Step 5: Identify and Document Controls

For each hazard, identify controls following the hierarchy of controls in Section 8. Document each control clearly. For standard operational assessments, review the default controls provided. For project-specific assessments, complete all control fields.

Step 6: Assess Residual Risk

Re-assess the risk for each hazard with all identified controls in place. The residual risk score must demonstrate a meaningful reduction from the inherent score. If the residual risk remains High or Critical, escalate per Section 7.4.

Step 7: Review and Approve

The completed risk assessment shall be reviewed and approved by the Group Compliance Director (or QHSE Manager when appointed) before the assessment is issued and before the assessed activity commences. Approval confirms that the methodology has been correctly applied, controls are adequate, and residual risks are ALARP.

Step 8: Communicate to Affected Personnel

All personnel affected by the risk assessment shall be briefed on the identified hazards, controls, and their individual responsibilities. Briefings shall be recorded. For vessel-based operations, this forms part of the pre-deployment or pre-embarkation safety briefing.

Step 9: Record and Monitor

The completed and approved risk assessment shall be filed in the management system (03 — Risk Assessments folder), registered in the Document Register (SM/INT/REG/001), and monitored for ongoing effectiveness. Any failure of controls or change in conditions triggers a review per Section 9.1.

11. REVIEW AND MONITORING

Risk assessments are living documents. They shall be reviewed and updated whenever triggered (Section 9.1) and at the scheduled frequency recorded in the Document Register.

The effectiveness of controls shall be monitored through:

- Incident and near-miss data from the Emergent HSE App
- Internal audit findings (SM/INT/PRO/003)
- Worker feedback and consultation
- Management review outputs
- Operational debrief reports

Where monitoring reveals that controls are ineffective or that risk levels have changed, the risk assessment shall be updated and reissued. Persistent control failures shall be raised as non-conformances under SM/INT/PRO/001.

12. RECORDS AND DOCUMENT CONTROL

The following records shall be maintained in accordance with the Control of Documents procedure (SM/INT/PRO/002):

- All completed risk assessments (RA-003 series), including superseded versions
- Evidence of risk assessment briefings delivered to personnel
- Records of risk assessment reviews, including the rationale for any changes
- Incident and near-miss reports that triggered risk assessment reviews
- Approval records (sign-off by the Group Compliance Director or QHSE Manager)

Risk assessments shall be retained for a minimum of three years after they are superseded or the operation they relate to has concluded, whichever is later.

13. RELATIONSHIP WITH SECURITY RISK ASSESSMENT

This procedure covers OH&S risks — those relating to injury, ill-health, and occupational safety. Security threats, geopolitical risks, business continuity risks, and reputational risks are assessed under SM/SEC/PRO/001 (Security and Business Risk Assessment Procedure) using the RA-004 methodology.

The boundary between the two procedures is as follows:

- OH&S (this procedure, RA-003): Physical injury, ill-health, occupational disease, fatigue, environmental exposure, equipment-related injury, workplace safety.
- Security (SM/SEC/PRO/001, RA-004): Armed attack, piracy, hijacking, terrorism, geopolitical threat, sanctions risk, reputational damage, contractual/legal liability.

Some activities present both OH&S and security risks. A vessel boarding in a high-threat area, for example, involves both physical safety hazards (pilot ladder transfer, equipment handling) and

security threats (armed confrontation, piracy). In such cases, both assessments apply. The RA-003 covers the safety dimension, the RA-004 covers the security dimension, and both are required before the operation is approved.

Where a risk assessment identifies a hazard that falls outside the scope of this procedure (i.e., it is a security or business risk rather than an OH&S risk), it shall be referred to the Group Compliance Director for assessment under SM/SEC/PRO/001.