SECURITY AND BUSINESS RISK ASSESSMENT PROCEDURE

SM/SEC/PRO/001 – Version 1.0

Security and Business Risk Assessment Procedure

Document Title	Security and Business Risk Assessment Procedure
Document Ref	SM/SEC/PRO/001
Version	1.0
Date Issued	1 April 2026
System	Security Management System (ISO 18788, ISO 28007, ISO 28000)
Classification	Internal
Review Date	April 2027
Approved By	Pavel Shparber, CEO
Prepared By	Darren Watts, Group Compliance Director
Supersedes	New document

1. PURPOSE

This procedure defines the process for identifying, assessing, and managing security and business risks across all Seagull Maritime operations. It establishes the framework for the RA-004 risk assessment pattern, which addresses threats across political, economic, social, technological, legal, and environmental (PESTLE) dimensions.

This procedure applies to risks arising from the external operating environment, client relationships, regulatory requirements, geopolitical factors, and business decisions. It complements the Hazard Identification and Risk Assessment Procedure (SM/HSE/PRO/001) which addresses occupational health and safety risks.

For new engagements, clients, regions, or material changes to existing operations, the Risk Screening Tool (SM/INT/DOC/003) must be completed before initiating a formal risk assessment under this procedure. The screening tool determines whether a formal assessment is required and which type.

2. SCOPE

This procedure applies to all Seagull Maritime entities including Seagull Malta, Seagull Dubai (FZCo), Seagull Offshore, and operations conducted under the Seagull Maritime flag across all operating regions.

It covers security risk assessments for maritime security operations (embarked teams, vessel protection), regional operational risk assessments (IOR, WAF/GOG, Persian Gulf, and any new theatre), client and contract risk assessments, vessel and flag state risk assessments, business continuity and reputational risk assessments, and regulatory and legal compliance risk assessments.

This procedure does not cover occupational health and safety hazard assessments (covered by SM/HSE/PRO/001) or routine operational risk assessments where no security or business dimension exists.

3. REFERENCES

- ISO 18788:2015 – Management system for private security operations
- ISO 28007-1:2015 – Ships and marine technology – Private maritime security companies
- ISO 28000:2022 – Security and resilience – Security management systems
- ISO 31000:2018 – Risk management – Guidelines
- BMP-MS – Best Management Practices – Maritime Security (replaces withdrawn BMP5)
- MISTO – Maritime Industry Shipping Threat Overview
- SM/HSE/PRO/001 – Hazard Identification and Risk Assessment Procedure
- SM/INT/DOC/003 – Risk Screening Tool – Concept and Design Specification
- SM/INT/PRO/001 – NCR, OFI and CAPA Management Procedure

4. DEFINITIONS

PESTLE Analysis – A framework for analysing Political, Economic, Social, Technological, Legal, and Environmental factors affecting operations.

Threat – Any potential source of harm to the organisation, its personnel, clients, or operations arising from the external environment.

Vulnerability – A weakness in the organisation's defences, procedures, or arrangements that could be exploited by a threat.

Risk – The combination of the likelihood of a threat exploiting a vulnerability and the severity of the resulting consequences.

Consequence Categories – The six sub-categories used to assess impact: Operational, Financial, Reputational, Legal/Regulatory, Personnel Safety, and Strategic.

Inherent Risk – The level of risk before the application of any controls or mitigation measures.

Residual Risk – The level of risk remaining after controls and mitigation measures have been applied.

Risk Appetite – The level of risk the organisation is willing to accept in pursuit of its objectives.

RA-004 Pattern – Seagull Maritime's standardised security and business risk assessment template using PESTLE analysis and multi-consequence scoring.

Risk Screening Tool – The pre-assessment gateway (SM/INT/DOC/003) that determines whether a formal risk assessment is required for new engagements.

5. ROLES AND RESPONSIBILITIES

5.1 Group Compliance Director (GCD)

- Owns this procedure and the security risk assessment framework
- Conducts or commissions all security and business risk assessments
- Reviews and approves completed assessments
- Maintains the risk assessment library
- Updates the conflict zone threat layer used by the Risk Screening Tool
- Determines risk appetite in consultation with the CEO

5.2 CEO

- Approves the risk appetite framework
- Reviews risk assessments for strategic decisions
- Endorses the Risk Screening Tool as mandatory for new engagements

5.3 Commercial Team (CCO)

- Completes the Risk Screening Tool for all new client enquiries and bids
- Provides client and contract information required for risk assessment
- Does not proceed with contractual commitment until screening or assessment is cleared

5.4 Operations Managers

- Completes the Risk Screening Tool for new taskings, vessel changes, or route changes
- Provides operational intelligence and threat information to support assessments
- Implements controls identified in completed risk assessments

5.5 Project Teams

- Complete the controls section of project-specific risk assessments (RA-004 pattern)
- Controls are left blank by design — the Project Team must populate them before task approval

5.6 All Personnel

- Report changes in operating conditions that may affect existing risk assessments
- Follow controls and mitigation measures identified in relevant assessments

6. THREAT IDENTIFICATION – PESTLE FRAMEWORK

Security and business threats are identified using the PESTLE framework. Each factor is analysed in the context of the specific operation, region, client, and contract.

6.1 Political

Government stability, regime change, political violence, sanctions regimes, diplomatic relations, military posture, port state requirements, flag state regulations, bilateral agreements, and coalition operations affecting the operating area.

6.2 Economic

Currency stability, insurance market conditions (war risk, P&I, H&M), fuel costs, local market conditions, client financial stability, payment terms, contract enforceability, and economic sanctions affecting trade routes or partners.

6.3 Social

Local population attitudes, tribal and ethnic dynamics, organised crime, piracy networks, civil unrest, labour relations, cultural factors affecting operations, media scrutiny, and NGO activity in the operating area.

6.4 Technological

Communications infrastructure, surveillance and monitoring capabilities, adversary technology (drones, GPS spoofing, cyber threats), vessel tracking systems, equipment reliability, and information security requirements.

6.5 Legal

Applicable maritime law, weapons licensing and carriage regulations, use of force frameworks, flag state requirements, port state control, data protection, employment law across jurisdictions, contractual liability, and insurance compliance requirements.

6.6 Environmental

Weather patterns, sea states, tidal conditions, visibility, temperature extremes, natural disaster risk, climate-related disruption to shipping routes, and environmental regulations affecting operations.

7. RISK ASSESSMENT METHODOLOGY – RA-004 PATTERN

The RA-004 pattern is Seagull Maritime's standardised framework for security and business risk assessment. It differs from the RA-003 (health and safety) pattern in three key ways: it uses PESTLE-based threat identification rather than hazard-based identification, it assesses consequences across six sub-categories which are averaged to produce the overall consequence score, and controls are left blank for the Project Team to complete.

7.1 Consequence Assessment

Each identified threat is assessed against six consequence sub-categories. Each sub-category is scored independently on a 1-5 scale. The overall consequence score is the average of all six sub-categories, rounded to the nearest whole number.

CATEGORY	FOCUS	ASSESSMENT CONSIDERS
Operational	Service delivery and capability	Impact on ability to deliver contracted services, operational disruption, equipment loss, mission failure
Financial	Direct and indirect costs	Contract losses, insurance claims, legal costs, compensation, equipment replacement, business interruption
Reputational	Stakeholder confidence	Client confidence, industry standing, media coverage, due diligence outcomes, certification body perception
Legal/Regulatory	Compliance and liability	Regulatory sanctions, licence revocation, criminal liability, civil claims, flag state action, certification risk
Personnel Safety	Physical harm to people	Injury or death to Seagull personnel, client crew, or third parties arising from security or business failures
Strategic	Long-term business impact	Market access, client relationships, competitive position, insurance availability, certification maintenance

7.2 Likelihood Assessment

Likelihood is assessed on a 1-5 scale.

LEVEL	DESCRIPTOR	INTERPRETATION
1	**Rare**	Conceivable but not expected in the foreseeable future. No known precedent in similar operations.
2	**Unlikely**	Could occur in exceptional circumstances. Limited precedent exists.
3	**Possible**	Has occurred before in similar operations or regions. Could occur during the life of this contract.
4	**Likely**	Expected to occur at some point. Regular occurrence in the operating area or sector.
5	**Almost Certain**	Expected to occur frequently or imminently. Active, current, and confirmed threat.

7.3 Risk Rating Matrix

The risk score is calculated as: Consequence (averaged) × Likelihood = Risk Score. The 5×5 matrix below uses colour coding to indicate risk levels.

	L=1	L=2	L=3	L=4	L=5
C=5	**5**	**10**	**15**	**20**	**25**
C=4	**4**	**8**	**12**	**16**	**20**
C=3	**3**	**6**	**9**	**12**	**15**
C=2	**2**	**4**	**6**	**8**	**10**
C=1	**1**	**2**	**3**	**4**	**5**

7.4 Risk Tolerance

RATING	TOLERANCE	MANAGEMENT APPROACH
LOW (1–4)	**Acceptable**	Monitor through normal operations. No additional controls required unless cost-effective.
MODERATE (5–9)	**Tolerable**	Manage through existing controls. Review at next scheduled assessment. Consider additional measures.
HIGH (10–16)	**Unacceptable without controls**	Formal controls required before proceeding. GCD approval needed. Enhanced monitoring.
CRITICAL (17–25)	**Unacceptable**	Operation must not proceed without CEO and GCD review and explicit approval. Maximum controls applied. Continuous monitoring.

8. CONTROLS AND RISK TREATMENT

Unlike health and safety risk assessments (RA-003 pattern), security and business risk assessments under the RA-004 pattern leave the controls section blank. This is a deliberate design decision. The Project Team responsible for the specific operation must identify, document, and implement controls before the task is approved. This creates an evidence trail demonstrating that the people executing the operation have actively considered and committed to specific risk mitigation measures. The GCD reviews all completed controls for adequacy.

Controls should follow the hierarchy: Avoid (do not accept the engagement), Transfer (insurance, contractual allocation), Reduce (procedural, physical, and administrative controls), Accept (accept residual risk with monitoring).

9. WHEN TO CONDUCT SECURITY RISK ASSESSMENTS

A formal security and business risk assessment is required when the Risk Screening Tool (SM/INT/DOC/003) returns an AMBER or RED rating, when entering a new operating region not covered by an existing RA-004, when engaging a new client in a sector Seagull has not previously served, when a material change occurs to an existing operation (new vessel, route change, contract scope change, personnel structure change), when the conflict zone threat assessment changes significantly for an active operating area, when directed by the GCD, CEO, or a client due diligence requirement, and when an incident, near-miss, or non-conformance indicates that the existing risk assessment is no longer adequate.

Existing risk assessments should be reviewed annually or when triggered by the conditions above. Routine operations covered by current, reviewed risk assessments do not require re-assessment unless circumstances change.

10. RISK ASSESSMENT PROCESS

The following ten-step process defines how security and business risk assessments are conducted.

Step 1 – Screening

Complete the Risk Screening Tool (SM/INT/DOC/003). If the result is GREEN, existing risk assessments apply and no new assessment is required. If AMBER or RED, proceed to Step 2.

Step 2 – Scope Definition

Define the scope of the assessment including the operation, region, client, vessel, contract period, and personnel involved. Determine which PESTLE factors are relevant.

Step 3 – Intelligence Gathering

Gather current threat intelligence from UKMTO advisories, MSCHOA updates, IMB piracy reports, NATO shipping centre alerts, BMP-MS guidance, MISTO assessments, the Seagull conflict zone monitoring output, and any client-provided information.

Step 4 – Threat Identification

Identify specific threats using the PESTLE framework (Section 6). Document each threat with a clear description of the threat source, mechanism, and potential impact.

Step 5 – Risk Scoring

Assess each threat against the six consequence sub-categories (Section 7.1) and likelihood (Section 7.2). Calculate the risk score using the matrix (Section 7.3).

Step 6 – Controls

For standard regional assessments, the GCD populates recommended controls. For project-specific assessments, the Project Team completes the controls section. All controls must be documented, assigned, and achievable.

Step 7 – Residual Risk

Re-score each threat with controls applied to determine the residual risk level.

Step 8 – Approval

The GCD reviews and approves the completed assessment. CRITICAL-rated residual risks require CEO review.

Step 9 – Communication

Distribute relevant Basic Risk Assessment Guides (BRAGs) to all affected personnel. Ensure operational teams understand the key risks and controls.

Step 10 – Monitoring

Monitor the operating environment throughout the contract period. Update the assessment when conditions change.

11. RELATIONSHIP WITH HEALTH AND SAFETY RISK ASSESSMENT

This procedure operates alongside SM/HSE/PRO/001 (Hazard Identification and Risk Assessment Procedure). The two procedures address different risk dimensions and use different assessment patterns (RA-004 for security/business, RA-003 for health and safety), but they share a common entry point through the Risk Screening Tool.

Where an operation requires both security/business and health and safety risk assessments, both must be completed before the operation is approved. The GCD coordinates across both procedures to ensure consistency and avoid gaps.

12. REVIEW AND MONITORING

This procedure is reviewed annually or when triggered by significant changes to the threat environment, operating regions, ISO standard requirements, client or certification body feedback, or non-conformance reports indicating procedural inadequacy.

The risk assessment library is reviewed quarterly by the GCD to ensure all active operations have current, valid assessments. The conflict zone threat layer feeding the Risk Screening Tool is updated daily as part of the GCD's monitoring routine.

13. RECORDS AND DOCUMENT CONTROL

All completed risk assessments are stored in the Seagull Maritime Management System under 03 - Risk Assessments/RA-004 Series. The Document Register (SM/INT/REG/001) tracks all risk assessment documents. The NCR/OFI/CAPA Register (SM/INT/REG/004) tracks any findings arising from risk assessment reviews. Screening tool outputs are retained as evidence of the pre-assessment process.

14. DOCUMENT HISTORY

VERSION	DATE	AUTHOR	DESCRIPTION
1.0	1 April 2026	Darren Watts, GCD	Initial release.