CUSTOS MARITIME & DEFENCE INDUSTRIES AB

Anti-Money Laundering and Counter-Terrorism Financing

Policy and Procedures

Document Owner:	Chief Financial Officer
Approved By:	Board of Directors
Effective Date:	1 January 2026
Review Frequency:	Annual
Version:	1.0

Table of Contents

1. Purpose and Scope

1.1 Purpose

This Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy establishes the framework for Custos Maritime & Defence Industries AB ("Custos" or the "Company") to prevent, detect, and report money laundering and terrorism financing activities. The Policy demonstrates the Company's commitment to operating with the highest standards of legal and regulatory compliance.

As a company listed on Euronext Growth Oslo and operating in the maritime and defence sectors, Custos recognizes its enhanced obligations under applicable AML/CTF regulations and the elevated risk profile of its business activities.

1.2 Scope

This Policy applies to:

- All directors, officers, employees, and contractors of Custos Maritime & Defence Industries AB and its subsidiaries, and any future acquisitions
- All business relationships with customers, suppliers, contractors, joint venture partners, and other third parties
- All jurisdictions in which the Company operates, including Norway, Sweden, and international operations
- All transactions, regardless of value, with enhanced scrutiny for high-value or high-risk transactions

1.3 Regulatory Framework

This Policy is designed to ensure compliance with:

- The Norwegian Money Laundering Act (Hvitvaskingsloven)
- The Norwegian Money Laundering Regulations (Hvitvaskingsforskriften)
- EU Fifth Anti-Money Laundering Directive (5AMLD)
- Financial Action Task Force (FATF) Recommendations
- Euronext Growth Market Rules and corporate governance requirements
- Applicable Swedish regulations for the parent company
- International sanctions regimes (UN, EU, US OFAC, and others)

2. Key Definitions

Money Laundering: The process of concealing the origins of illegally obtained money, typically by means of transfers involving legitimate businesses or foreign banks.

Terrorism Financing: The provision or collection of funds with the intention or knowledge that they are to be used to carry out terrorist acts.

Customer Due Diligence (CDD): The process of identifying and verifying the identity of customers and assessing the risk they pose for money laundering or terrorism financing.

Enhanced Due Diligence (EDD): Additional measures applied to higher-risk customers, transactions, or business relationships beyond standard CDD.

Politically Exposed Person (PEP): An individual who is or has been entrusted with prominent public functions, including heads of state, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations, and important political party officials.

Beneficial Owner: The natural person(s) who ultimately owns or controls a legal entity or on whose behalf a transaction is being conducted, typically defined as those holding more than 25% ownership or control.

Suspicious Activity: Any transaction or activity that gives reasonable grounds to suspect that it involves proceeds from criminal activity or is related to terrorism financing.

High-Risk Jurisdiction: Countries or territories identified by FATF or other international bodies as having strategic AML/CTF deficiencies or being subject to international sanctions.

3. Governance and Responsibilities

3.1 Board of Directors

The Board of Directors has ultimate responsibility for:

- Approving and overseeing the AML/CTF Policy and framework
- Ensuring adequate resources are allocated for AML/CTF compliance
- Reviewing annual AML/CTF risk assessments and compliance reports
- Establishing a culture of compliance throughout the organization

3.2 Chief Compliance Officer (CCO)

The CCO serves as the designated AML/CTF Compliance Officer and is responsible for:

- Day-to-day oversight of the AML/CTF program
- Implementing and maintaining AML/CTF policies and procedures
- Conducting or coordinating risk assessments
- Serving as the primary contact with regulatory authorities
- Reviewing and approving high-risk customer relationships
- Investigating suspicious activity reports
- Coordinating AML/CTF training programs
- Preparing and submitting required regulatory reports

3.3 Management and Department Heads

Department heads and senior management are responsible for:

- Implementing AML/CTF policies within their respective areas
- Ensuring staff receive appropriate AML/CTF training
- Monitoring transactions and activities for suspicious behavior
- Escalating concerns to the AML/CTF Compliance Officer
- Maintaining appropriate records and documentation

3.4 All Employees

Every employee, contractor, and representative of Custos must:

- Understand and comply with this AML/CTF Policy
- Complete mandatory AML/CTF training
- Report any suspicious activity or potential violations
- Cooperate fully with internal and external AML/CTF investigations

3.5 Internal Audit

The Internal Audit function (or external auditors where internal audit does not exist) will conduct periodic independent reviews of the AML/CTF program to assess its effectiveness and compliance with regulatory requirements. Audit findings and recommendations will be reported to the Board's Audit Committee.

4. Risk Assessment

4.1 Enterprise-Wide Risk Assessment

Custos conducts a comprehensive AML/CTF risk assessment at least annually to identify, assess, and understand the money laundering and terrorism financing risks it faces. The risk assessment considers:

- **Customer risk:** Types of customers, their business activities, ownership structures, and geographical locations
- **Country and geographic risk:** Jurisdictions in which the Company operates and those of customers and suppliers
- **Product and service risk:** Shipbuilding, repair, defence manufacturing, and related services offered
- **Transaction and delivery channel risk:** Payment methods, transaction sizes, and business delivery mechanisms
- **Industry-specific risks:** Maritime and defence sectors' unique vulnerabilities to illicit finance

4.2 Sector-Specific Risks: Maritime and Defence

Custos acknowledges the heightened AML/CTF risks inherent in the maritime and defence sectors:

Maritime Sector Risks

- High-value transactions typical in shipbuilding and repair
- Complex ownership structures common in vessel registration
- Use of flags of convenience and offshore jurisdictions
- Cash-intensive operations in some maritime markets
- Potential involvement with sanctioned entities or jurisdictions
- Trade-based money laundering through shipping activities

Defence Sector Risks

- Transactions involving military and dual-use technologies
- Government and military end-users
- Potential diversion of defence materials to unauthorized parties
- Complex international supply chains
- Strict export control and sanctions compliance requirements
- Politically exposed persons as potential customers or partners

4.3 Risk Mitigation Measures

Based on the identified risks, Custos implements appropriate risk-based controls, including:

- Enhanced due diligence for high-risk customers and transactions
- Rigorous beneficial ownership verification procedures
- Comprehensive sanctions screening protocols
- Transaction monitoring and review processes
- Regular training on maritime and defence sector-specific red flags
- Close coordination with export control and sanctions compliance functions

5. Customer Due Diligence

5.1 Standard Customer Due Diligence

Before establishing a business relationship or conducting a transaction exceeding EUR 15,000, Custos will conduct Customer Due Diligence (CDD) procedures to:

- Identify and verify the customer's identity using reliable, independent source documents, data, or information
- Identify the beneficial owner(s) and take reasonable measures to verify their identity
- Understand and obtain information on the purpose and intended nature of the business relationship
- Conduct ongoing monitoring of the business relationship and transactions

5.1.1 Corporate Customer Requirements

For legal entities, CDD must include:

- Certificate of incorporation or equivalent registration document
- Articles of association or equivalent founding documents
- Register of shareholders and beneficial owners
- Register of directors and authorized signatories
- Business license or regulatory approvals (where applicable)
- Proof of registered address
- Financial statements or other evidence of business operations
- Identification documentation for beneficial owners holding 25% or more ownership or control

5.1.2 Individual Customer Requirements

For individual customers, CDD must include:

- Valid government-issued photo identification (passport, national ID card, or driver's license)
- Proof of residential address (utility bill, bank statement, or government correspondence)
- Information on source of funds and source of wealth for high-value transactions
- Business or occupation information

5.2 Enhanced Due Diligence

Enhanced Due Diligence (EDD) must be conducted for higher-risk situations, including but not limited to:

- Politically Exposed Persons (PEPs), their family members, and close associates
- Customers or transactions involving high-risk jurisdictions
- Complex ownership structures or nominee arrangements
- Transactions or relationships with unusual circumstances or characteristics
- Cash-intensive businesses
- Non-face-to-face customer relationships
- Correspondent banking relationships
- Defence contracts with foreign government end-users
- Vessel registration in offshore or high-risk jurisdictions

5.2.1 Enhanced Due Diligence Measures

EDD procedures include:

- Obtaining additional information on the customer, beneficial owners, and business activities
- Obtaining information on the source of funds and source of wealth
- Obtaining senior management approval for establishing or continuing the business relationship
- Conducting enhanced ongoing monitoring of the relationship

- Requesting additional documentation and conducting independent verification
- Conducting adverse media checks and reputation due diligence
- More frequent reviews and updates of customer information
- Additional scrutiny of payment patterns and transaction structures

5.3 Simplified Due Diligence

Simplified due diligence may be applied in limited low-risk situations, such as with customers that are:

- Norwegian or EU public authorities
- Listed companies subject to regulatory disclosure requirements
- Financial institutions authorized in Norway, EU, or equivalent jurisdictions
- However, given the maritime and defence sectors' elevated risk profile, simplified due diligence should be applied cautiously and only with AML/CTF Compliance Officer approval.

5.4 Ongoing Monitoring

Custos maintains ongoing monitoring of all customer relationships, including:

- Scrutinizing transactions to ensure they are consistent with the customer profile and business relationship
- Keeping customer information and documentation up to date
- Reviewing customer risk classifications at least annually or when triggered by specific events
- Conducting periodic reviews of high-risk relationships (at least annually)

5.5 Timing of Verification

Customer identity verification must be completed before establishing the business relationship or conducting the transaction. In limited circumstances, verification may be completed during establishment if:

- Necessary to avoid interrupting normal business conduct
- Money laundering and terrorism financing risks are effectively managed
- Verification is completed as soon as practicable thereafter

6. Sanctions Screening

6.1 Screening Requirements

Custos maintains and implements a comprehensive sanctions screening program to prevent transactions or relationships with sanctioned individuals, entities, or jurisdictions. All customers, vendors, business partners, and beneficial owners must be screened against:

- United Nations Security Council sanctions lists
- European Union sanctions lists
- US Office of Foreign Assets Control (OFAC) sanctions lists
- UK HM Treasury sanctions lists
- Norwegian and Swedish national sanctions lists
- PEP lists and databases
- Adverse media databases

6.2 Screening Timing

Screening must be conducted:

- Before establishing any new business relationship
- Before conducting any transaction
- On an ongoing basis for existing relationships (at least quarterly)
- When sanctions lists are updated
- When there are material changes in customer information

6.3 Handling Screening Matches

Any screening match (potential or confirmed) must be immediately escalated to the AML/CTF Compliance Officer. No transaction may proceed until the match is resolved. If a true match is confirmed:

- The business relationship must be terminated or the transaction rejected
- Any funds held must be frozen pending further instructions from authorities
- Competent authorities must be notified as required by applicable regulations
- Legal counsel should be consulted on appropriate remedial actions

7. Suspicious Activity Reporting

7.1 Reporting Obligation

Any employee who knows, suspects, or has reasonable grounds to suspect that a transaction or activity involves proceeds from criminal activity or is related to money laundering or terrorism financing must immediately report their concerns to the AML/CTF Compliance Officer.

7.2 Red Flags and Indicators

While not exhaustive, the following are examples of suspicious activity indicators relevant to Custos's operations:

General Red Flags

- Customer reluctance to provide required information or documentation
- Provision of suspicious, false, or difficult to verify documentation
- Unusual or excessively complex ownership structures without commercial rationale
- Customer transactions inconsistent with stated business purpose or financial profile
- Unexplained changes in transaction patterns or account activity
- Frequent changes in beneficial ownership or corporate structure
- Use of shell companies or entities with no apparent business purpose

Maritime-Specific Red Flags

- Vessels registered in jurisdictions with weak regulatory oversight
- Frequent changes in vessel registration or flag
- Complex nominee arrangements obscuring true vessel ownership
- Payment from or to jurisdictions unconnected to the vessel or customer
- Requests for unusual payment arrangements or anonymity
- Vessel operations or routes inconsistent with stated business purpose
- Customer evasiveness about vessel cargo or destinations

Defence-Specific Red Flags

- Customer or end-user located in high-risk or sanctioned jurisdiction
- Unusual requests for technical specifications or capabilities
- Requests to obscure end-use or end-user information
- Involvement of intermediaries with no clear commercial purpose

- Attempts to avoid export control or licensing requirements
- Customer or project associated with adverse media related to conflict or arms trafficking
- Requests for modifications that could have military applications

Payment-Related Red Flags

- Payments from third parties unrelated to the customer
- Payments to or from high-risk jurisdictions
- Unusual use of cash or cash equivalents
- Structuring of payments to avoid reporting thresholds
- Significant overpayments followed by refund requests
- Wire transfers from multiple sources or through multiple jurisdictions
- Requests for payments to be made to accounts in different names or jurisdictions

7.3 Internal Reporting Process

When suspicious activity is identified, the following process must be followed:

1. Employee documents concerns and immediately reports to their supervisor and the AML/CTF Compliance Officer
2. AML/CTF Compliance Officer reviews the report and conducts preliminary investigation
3. If suspicion is substantiated, AML/CTF Compliance Officer determines whether a Suspicious Transaction Report (STR) must be filed with Økokrim (Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime)
4. If required, STR is filed without delay and without informing the customer
5. Decision on whether to continue, suspend, or terminate the business relationship is made by senior management in consultation with legal counsel
6. All actions and decisions are documented in the AML/CTF compliance file

7.4 Prohibition on Tipping Off

No person may disclose to a customer or any other unauthorized person that a suspicious activity report has been filed or that an investigation is underway. Such disclosure ("tipping off") is a criminal offence and may result in prosecution.

7.5 Protection for Whistleblowers

Employees who report suspicious activity in good faith are protected from retaliation. No adverse employment action will be taken against any employee for making a good faith report of suspected money laundering or terrorism financing, even if the report is ultimately determined to be unfounded.

8. Record Keeping

8.1 Retention Requirements

Custos maintains comprehensive records in accordance with Norwegian legal requirements. All records must be kept for at least five years after:

- The completion of the transaction, or
- The end of the business relationship

8.2 Required Records

Records that must be maintained include:

- Customer identification and verification documentation
- Beneficial ownership information and verification
- Risk assessments and risk ratings
- Transaction records and supporting documentation
- Sanctions screening results
- Suspicious activity reports and internal investigations
- Training records
- Correspondence with customers regarding AML/CTF matters
- Internal AML/CTF policies, procedures, and audits
- Records of decisions not to proceed with customers or transactions

8.3 Record Format and Accessibility

Records may be kept in paper or electronic format but must be:

- Complete and accurate
- Readily accessible and retrievable
- Protected from unauthorized access, alteration, or destruction
- Available for inspection by regulatory authorities upon request

8.4 Data Protection

All AML/CTF records containing personal data must be processed in compliance with the General Data Protection Regulation (GDPR) and applicable Norwegian data protection laws. Access to AML/CTF records should be restricted to authorized personnel only.

9. Training and Awareness

9.1 Training Requirements

All employees, directors, and relevant contractors must receive regular AML/CTF training appropriate to their roles and responsibilities. Training must be provided:

- During onboarding for new employees
- At least annually for all staff
- When there are material changes to policies, procedures, or regulations
- When employees assume new roles with AML/CTF responsibilities

9.2 Training Content

Training programs must cover:

- Overview of money laundering and terrorism financing risks
- Relevant laws, regulations, and regulatory requirements
- Company AML/CTF policies and procedures
- Customer due diligence requirements and procedures
- Recognition of suspicious activity and red flags
- Sanctions screening and compliance
- Reporting procedures and requirements
- Record-keeping requirements
- Maritime and defense sector-specific risks and typologies
- Consequences of non-compliance

9.3 Enhanced Training

Employees in high-risk positions (sales, customer service, finance, compliance, senior management) receive enhanced training tailored to their specific responsibilities and the risks they are likely to encounter.

9.4 Training Records

Records of all AML/CTF training must be maintained, including participant names, dates, topics covered, and attendance confirmation. Training effectiveness should be periodically assessed through testing or other evaluation methods.

10. Third Party Relationships

10.1 Agents and Intermediaries

When Custos engages agents, intermediaries, or other third parties who will interact with customers or conduct business on the Company's behalf, due diligence must be conducted on these parties. This includes:

- Verification of identity and business legitimacy
- Assessment of AML/CTF risks and controls
- Verification of regulatory licenses and good standing
- Reputation checks and adverse media screening
- Written agreements requiring compliance with AML/CTF standards
- Periodic monitoring and re-evaluation of the relationship

10.2 Reliance on Third Parties

Custos may rely on third parties (such as banks, law firms, or accounting firms) to conduct elements of CDD, provided that:

- The third party is regulated for AML/CTF purposes in Norway, the EU, or an equivalent jurisdiction
- Custos obtains written confirmation that CDD has been performed
- Custos can obtain copies of identification data and other relevant documentation immediately upon request
- Ultimate responsibility for CDD remains with Custos

10.3 Joint Ventures and Partnerships

For joint ventures, partnerships, or consortium arrangements, Custos will:

- Conduct thorough due diligence on all partners
- Ensure AML/CTF obligations and responsibilities are clearly defined in agreements
- Assess partners' AML/CTF compliance programs
- Maintain oversight of the joint venture's AML/CTF compliance

11. Compliance Monitoring and Testing

11.1 Internal Audit

An independent audit of the AML/CTF program will be conducted at least annually by internal audit or qualified external auditors. The audit scope should include:

- Effectiveness of risk assessment processes
- Adequacy of customer due diligence procedures
- Compliance with sanctions screening requirements

- Quality of suspicious activity detection and reporting
- Adequacy of record-keeping
- Effectiveness of training programs
- Testing of a sample of customer files and transactions
- Overall governance and oversight of the AML/CTF program

11.2 Continuous Monitoring

The AML/CTF Compliance Officer implements continuous monitoring processes, including:

- Regular review of high-risk customer files
- Transaction monitoring and anomaly detection
- Sanctions list updates and rescreening
- Quality assurance reviews of CDD documentation
- Spot-checks of compliance with procedures

11.3 Reporting to Board

The AML/CTF Compliance Officer provides regular reports to the Board of Directors (at least annually) covering:

- Status of AML/CTF compliance program
- Results of risk assessments
- Statistics on suspicious activity reports
- Training completion rates
- Audit findings and remediation progress
- Regulatory developments and updates
- Recommendations for program improvements

12. Consequences of Non-Compliance

Failure to comply with this AML/CTF Policy may result in serious consequences for both the Company and individuals, including:

For the Company

- Criminal prosecution
- Substantial financial penalties
- Regulatory sanctions or license revocation
- Reputational damage
- Delisting from Euronext Growth Oslo
- Loss of business relationships and banking services

For Individuals

- Criminal prosecution and imprisonment
- Personal financial penalties
- Disciplinary action up to and including termination of employment
- Disqualification from serving as director or officer
- Damage to professional reputation and career

13. Policy Review and Updates

This AML/CTF Policy will be reviewed at least annually or more frequently if required by:

- Changes in applicable laws or regulations
- Changes in the Company's business activities, structure, or risk profile

- Results of internal audits or regulatory examinations
- Identified deficiencies or weaknesses in the program

Any material changes to the Policy must be approved by the Board of Directors and communicated to all relevant personnel.

14. Contact Information

Questions regarding this Policy or AML/CTF matters should be directed to:

AML/CTF Compliance Officer

Chief Compliance Officer

Custos Maritime & Defence Industries AB

Email: ve@custos-md.com

15. Approval and Acknowledgment

This Anti-Money Laundering and Counter-Terrorism Financing Policy has been approved by the Board of Directors of Custos Maritime & Defence Industries AB.

_____ Board Chairman	Date: _____
_____ Chief Executive Officer	Date: _____
_____ Chief Financial Officer / AML Compliance Officer	Date: _____

Appendix A: High-Risk Jurisdictions

The following categories of jurisdictions are considered high-risk for AML/CTF purposes. This list should be reviewed regularly and updated based on FATF and other authoritative sources:

A.1 FATF High-Risk Jurisdictions

Countries identified by FATF as having strategic AML/CTF deficiencies with which enhanced due diligence should be applied. The current list should be accessed at: www.fatf-gafi.org/countries/#high-risk

A.2 Sanctioned Jurisdictions

Countries subject to comprehensive economic sanctions by the UN, EU, US, or other relevant authorities, including but not limited to:

- North Korea (DPRK)
- Iran
- Syria
- Crimea and certain regions of Ukraine
- Cuba (US sanctions)
- Other jurisdictions as designated

A.3 Tax Havens and Offshore Financial Centers

Jurisdictions with weak transparency and beneficial ownership requirements, including certain Caribbean, Pacific Island, and other offshore centers. Enhanced scrutiny should be applied to entities registered in these locations.

A.4 Flags of Convenience

For maritime operations, particular attention should be paid to vessels registered under flags of convenience with weak regulatory oversight, including but not limited to certain registries in Belize, Comoros, Cambodia, and others identified by maritime authorities.

Note: *This appendix should be updated regularly by the AML/CTF Compliance Officer based on current FATF publications, EU regulations, and other authoritative sources.*

Appendix B: Customer Risk Rating Matrix

The following matrix provides guidance for assigning risk ratings to customers based on various risk factors. The final risk rating should consider all relevant factors and may be adjusted based on professional judgment.

Risk Factor	Low Risk	Medium Risk	High Risk
Geography	Norway, EU/EEA	Other developed markets	FATF-listed, sanctioned, or offshore jurisdictions
Customer Type	Public authorities, listed companies	Private companies, established businesses	Complex structures, shell companies, PEPs
Business Activity	Standard commercial shipping	Civil maritime services	Defence contracts, military end-users, high-value transactions

Transaction Volume	< EUR 1 million	EUR 1-10 million	> EUR 10 million

\nNote: *The final risk rating should be determined by the AML/CTF Compliance Officer considering all relevant factors. High-risk customers require Enhanced Due Diligence and senior management approval.*