

DJIBOUTI CODE OF CONDUCT (DCoC) ENGAGEMENT STRATEGY

EXECUTIVE SUMMARY

This Engagement Strategy consolidates the priorities, threats, opportunities, and actions facing DCoC States and partners in 2025. It is designed to serve as both a high-level policy narrative and a practical implementation tool, aligning with the draft Regional Maritime Security Strategy (RMSS). Its central message is clear: DCoC States must lead, while partners, donors, and industry support through coordinated mechanisms.

The Engagement Strategy is informed by the regional threat context and the strengths, weaknesses, opportunities and threats (SWOT) analysis as well as by the lessons and best practices identified during the consultation phase, including the need to better engage with States that are not fully participating in the DCoC programmes. It is guided by five principles: Sovereignty, regional ownership, Inclusivity, Investment and support partnership, and industry partnership. It outlines seven strategic priorities: Governance, operational cooperation, legal harmonization, coordination of support, industry engagement, resilience and gender and inclusion.

For clarity, this document distinguishes between National Maritime Security Committees (NMSCs), which are inter-ministerial bodies at national level, and National Maritime Information Sharing Centres (NMISCs), which are technical operational hubs for maritime domain awareness and reporting. The Capacity-Building Matrix (CB Matrix) is the online tool used to match State requirements with donor support, while the DCoC Trust Fund is the dedicated financial mechanism for sustaining agreed projects.

The Engagement Strategy also offers an action plan with key performance indicators and proposes next steps.

1 THREAT CONTEXT

The maritime threat environment in the Red Sea, Gulf of Aden (GoA), and Western Indian Ocean (WIO) has become increasingly complex. State-based threats, non-state armed groups, and transnational criminal networks intersect to challenge maritime security. This section provides a consolidated threat picture for DCoC States.

There are many sources of threat information including IMO's Global Integrated Shipping Information System (GISIS), INTERPOL, RMIFC/RCOC, international navies including CMF and EUNAVFOR, the International Maritime Bureau and others. These useful sources of information should be taken into account when developing and updating

national maritime security risk registers (NMSRRs); and establishing regional databases (e.g., vessels of interest) (RMSS §1.1.5.8). DCoC States should commit to a biennial DCoC-wide maritime threat assessment (RMSS §1.1.2).

1.1 Threat Matrices

Threat Category	Primary Areas	Key Indicators	Recommended Operator Actions
Conflict-linked attacks (Houthi)	Southern Red Sea, Bab al-Mandeb	UAV/missile/USV alerts; AIS/GPS interference; traffic patterns around Hodeidah	Follow BMP-MS hardening, convoy where available (ASPIDES/CMF), maintain 24/7 reporting to UKMTO/MSC-HOA
Piracy / Armed Robbery	GoA TSS; WIO off Somalia (300–600 NM offshore)	Dhows/fishing vessels shadowing, no gear; sudden approach at speed	BMP-MS measures (citadel, razor wire, water cannons); maintain reporting; adhere to IRTC routes
IUU Fishing	WIO EEZs, Somali & Mozambican banks	Foreign fishing vessels with poor docs, no observers, reefers STS transfers	Verify flag & licenses; PSC checks; support regional RFMO/IOTC port-state controls
Illegal Wildlife Trade (IWT)	East Africa → Gulf/Asia container routes	Timber/ivory/pangolin/turtles concealed in “timber/seafood/plastic” consignments	Heightened cargo screening; intelligence sharing with customs/environment units
Drugs (“Southern Route”)	Arabian Sea / GoA dhow lanes	Dhows with hidden compartments, irregular routing; interdiction intelligence from CMF	Support CTF-150 patrols; notify on suspect dhows; ensure chain-of-custody procedures
Weapons Smuggling (UN sanctions)	Iran → Yemen routes; Somalia arms embargo	Dhow convoys; concealed weapons systems; falsified fishing papers	Interdiction under UNSC mandate; evidence preservation; coordinate with UN Panels of Experts
Human trafficking & migrant smuggling	Horn of Africa → Yemen; GoA crossings	Overloaded boats/dhows; no safety gear; clandestine departures	SAR readiness; humanitarian treatment; coordinate with IOM/UNHCR
Other illicit activity (fuel/oil theft, waste dumping)	Offshore anchorages, STS zones	Tankers with repeated STS ops, odd “waste” cargo declarations	Port-state inspection; monitor STS under MARPOL rules; report to IMO/UNEP

1.2 Risks & State Response Obligations to the Threats

The above-mentioned maritime threats imply corresponding response obligations required of DCoC Signatory States. These include measures against piracy resurgence, IUU fishing, smuggling (narcotics, arms, fuel, wildlife), human trafficking, and cyber threats. Each obligation set out below is aligned with the DCoC/JA provisions and reinforced by RMSS derived tasks.

Response Area	Expected State Action
Legislation & Criminalization	Enact laws covering piracy, armed robbery, IUU fishing, human/weapon/drug/wildlife trafficking, pollution crimes, in line with UNCLOS & conventions.
Maritime Domain Awareness (MDA)	Maintain/upgrade national & regional information-sharing centres (e.g., Dar es Salaam, Sana'a). Exchange incident reports, AIS data, intelligence on illicit flows.
Inter-agency coordination	Ensure cooperation between navies, coast guards, fisheries, customs, immigration, environment, and port authorities.
Capacity building	Train boarding teams (visit, board, search & seizure), evidence collection, crew welfare monitoring. Support joint exercises with CMF/EUNAVFOR/IMO.
Law enforcement at sea	Patrol EEZs and high seas (where authorized); interdict and detain vessels engaged in illicit acts; secure chain of evidence; ensure humane treatment of suspects & migrants.
Sanctions enforcement	Apply UNSC Somalia/Yemen regimes: prevent charcoal exports, weapons imports; board suspect dhows; report seizures to Sanctions Committees.
Fisheries management	Implement port-state measures against IUU; deny entry/landing to IUU-caught fish; cooperate with RFMOs (IOTC).
Humanitarian & human rights compliance	Provide SAR for migrants; coordinate with IOM/UNHCR; uphold human rights when detaining crews/suspects.
Regional cooperation	Actively participate in IMO/DCoC working groups; share best practice and lessons learned; contribute to capacity building for less resourced signatories.
Prosecution & judiciary	Develop prosecutorial capacity for complex maritime crimes (e.g., piracy, narcotics, IWT); enter into regional agreements for transfer of suspects.

1.3 Implications for DCoC

These threat patterns highlight the urgent need for regional coordination through the DCoC signatory States, especially through WG3, the operationalization of National Maritime Information Sharing Centres (NMISCs), and alignment of donor support via the

capacity building (CB) Matrix. States must harmonize legislation and commit operational assets to ensure legal finish and deterrence (RMSS §2.3.2.1; §1.1.6).

2 SWOT ANALYSIS

This SWOT analysis provides a clear view of strengths, weaknesses, opportunities, and threats facing DCoC States as they implement the Jeddah Amendment. Each factor is explained in narrative form and summarised in a structured table. Inline references to RMSS sections are included where relevant, with additional sources footnoted.

2.1 Strengths

The DCoC framework provides a unique multilateral platform for regional maritime security, anchored in the Jeddah Amendment (2017). With Working Groups 1–3 now functional, including the newly established WG3 on operational cooperation, States have an institutional vehicle for joint patrols, SAR coordination, and legal finish (RMSS §1.1.6). The creation of National Maritime Information Sharing Centres (NMISCs) in Kenya and Tanzania demonstrates progress towards decentralised information sharing and operational readiness. Investment and support partnership through the Capacity Building Matrix adds coherence, while political ownership by coastal States provides legitimacy.

2.2 Weaknesses

Despite institutional advances, political commitment remains uneven across signatories. Some States lack legal frameworks or dedicated maritime institutions, impeding harmonisation and undermining regional coherence (RMSS §2.3.2.1). Donor funding is fragmented, and the DCoC Trust Fund remains under-supported. Capacity gaps in ICT, staffing, and training continue to limit the effectiveness of NMISCs. Industry engagement is largely ad hoc, with confidentiality concerns limiting voluntary reporting. Limited female/youth participation in maritime security institutions.

2.3 Opportunities

WG3 provides a roadmap for operationalisation, including SOPs, exercises, and eventually a joint task force. This represents an opportunity to institutionalise practical cooperation at sea. A Public–Private Maritime Security Forum can bring industry stakeholders into the security architecture, ensuring alignment on reporting, cyber resilience, and Humanitarian Assistance and Disaster Response (HA/DR). The inclusivity agenda, including gender and youth mainstreaming, enhances legitimacy and opens access to additional funding streams. Regional synergies with SHADE, CMF, ATALANTA, AU, IORA, IONS and the Red Sea Council create a broader ecosystem for coordination. The opportunities for civil–military cooperation (joint MDA, liaison officers, PPP in maritime security, crisis response coordination) were identified as key in CMF/EUNAVFOR/KSA mission reports. Bahrain signing the DCoC brings further potential engagement with remaining GCC countries yet to sign.

2.4 Threats

The threat environment is deteriorating, with piracy indicators resurfacing in the WIO and GoA, alongside Houthi missile and UAV attacks in the Red Sea. Transnational organised crime, including IUU fishing, narcotics, and arms smuggling, undermines governance and security. Geopolitical rivalries risk fragmenting Investment and support partnership, while technological gaps leave States vulnerable to cyber and drone-enabled attacks. Sustainability is another concern, as progress may stall if donor support declines.

2.5 SWOT Summary Table

Strengths	Weaknesses
• Recognized DCoC/JA mandate • DCoC governance structure including WGs1,2 and 3 • WG3 roadmap • RMIFC/RCOC; • SHADE/CMF/ATALANTA • IORIS • Kenya & Tanzania NMISCs	• Variable commitment • legal gaps for NMISCs/NMSCs • fragmented reporting/calendars • donor duplication • cyber gaps • industry confidentiality concerns • lack of female/youth participation
Opportunities	Threats
• WG3 representation in SHADE • IORIS as standard • ISN routing SOP • Legal Forum & evidence SOP • RSC/PERSGA/Nairobi synergies • IORA/IONS • Public–Private Forum • Gender and youth mainstreaming • Civil/military cooperation • Engagement with GCC countries	• Piracy resurgence • Conflict spillover; • Geopolitics/donor volatility • cyber/EW • slow legal reform • tool fragmentation without SOPs

2.6 The SWOT analysis above highlights both the strengths of the DCoC framework and the urgent gaps that remain. These findings directly shape the strategic priorities set out in the next section. By moving from analysis to action, the Engagement Strategy ensures that lessons identified are translated into concrete, sequenced measures that strengthen regional ownership and coordination.

3 ENGAGEMENT STRATEGY

The Engagement Strategy provides the central storyline for how DCoC States, partners, and industry will collectively operationalize the Jeddah Amendment and draft Regional Maritime Security Strategy (RMSS). It moves beyond the framework of Ends, Ways, and Means, to set clear priorities, sequencing, and lines of effort. The strategy is underpinned by the principle that DCoC States must lead, with partners and donors enabling regional ownership and sustainability.

3.1 Strategic Aim

The aim of this strategy is to secure the maritime domain of the Red Sea, Gulf of Aden, and Western Indian Ocean by building resilient national and regional institutions, deterring piracy and transnational crime, and ensuring lawful, sustainable use of the seas. This is achieved by empowering DCoC States to lead, aligning partners and donors, and embedding inclusivity and resilience as cross-cutting principles.

3.2 Guiding Principles

The Engagement Strategy is guided by five principles:

1. Sovereignty – States retain primacy over their maritime zones and security responsibilities.
2. Regional Ownership – DCoC structures (including the Steering Committee, WGs1,2 and 3, the ISN, NMISCs) are the anchors for coordination.
3. Inclusivity – Gender, youth, and civil society participation mainstreamed across activities, with measurable targets.
4. Investment and support partnership – Funding and contributions-in-kind for capacity building activities coordinated via the CB Matrix and Trust Fund (RMSS §2.2.4.4).
5. Industry Partnership – Institutionalized through a Public–Private Maritime Security Forum.

3.3 Strategic Priorities

The strategy is structured around seven mutually reinforcing lines of effort. These correspond to the main Action Plan pillars, ensuring coherence between policy and implementation.

1. Governance – Establish NMSCs, strengthen coordination, mainstream inclusion (RMSS §2.3.2), requirement for NMSRRs (RMSS §1.1.2.4)..

2. Operational Cooperation – Implement WG3 roadmap, NMISCs, SOPs, and exercises (RMSS §1.1.6; §1.2.2.3), establish regional databases (vessels of interest, law enforcement detachments)
3. Legal Harmonization – Align national laws; establish Regional Legal Forum, address “legal finish” shortcomings (“catch and release”) (RMSS §2.3.2.1; §2.3.5).
4. Coordination of support – Annual donor roundtable; operationalise Trust Fund (RMSS §2.2.4.4; §2.2.4.7).
5. Industry Engagement – Launch Public–Private Forum; integrate voluntary reporting (RMSS §1.2.2.3).
6. Resilience – Develop cyber frameworks and protocols; conduct HA/DR exercises; assess critical infrastructure (RMSS §3.5.1; §3.4.3.5).
7. Gender and inclusion - Mainstream gender and youth across governance, operations, and capacity building; ensure at least 30% participation in national and regional maritime security structures and exercises by 2028; establish gender-sensitive training, mentorship, and recruitment pathways. (This element needs to be included in the draft RMSS).

3.4 Sequencing

The Engagement Strategy is phased to ensure that early wins build momentum and capacity for more complex tasks:

2025–2027: Foundations – Establish NMISCs, adopt ISN SOPs including for threat assessment, launch Public–Private Forum, align donors, engage with non-active signatory States.

2028–2030: Consolidation – Conduct regular WG3 exercises, harmonise national laws, operationalise Trust Fund, mainstream gender/youth, integrate industry reporting.

Beyond 2030: Resilience – Expand focus to HA/DR, environmental security, and critical infrastructure protection.

3.5 Stakeholder Engagement

3.5.1 Engagement with stakeholders is not an ancillary activity but a direct reflection of the guiding principle of inclusivity. By systematically involving signatory States, industry, civil society, and international partners, the strategy builds legitimacy and ensures that diverse voices are embedded into planning and implementation. This approach enhances transparency, accountability, and sustainability of outcomes.

3.5.2 Effective implementation requires targeted engagement with diverse stakeholders:

1. States – Provide leadership, legislate, staff national institutions, engage with inactive DCoC States and other potential partners.
2. Regional Centres – RMIFC and RCOC provide analysis, deconfliction, and coordination.
3. Investment and development partners – Fund or contribute in kind to capacity-building via the CB Matrix and Trust Fund.
4. Industry – Engage via the Public–Private Forum to provide reporting, share cyber practices, and support resilience planning.
5. Civil Society – Build legitimacy through inclusion, training, and community engagement.
6. International Partners – Coordinate naval presence via SHADE, CMF, ATALANTA, India, and regional bodies including AU, IGAD, IORA, IONS, GCC and regional Arab structures.

3.6 Regional Synergies

The Engagement Strategy aligns with regional and international initiatives to avoid duplication and leverage synergies. SHADE ensures deconfliction among navies. CMF and ATALANTA provide deterrence and tactical reach. The Red Sea Council, AU, IGAD, and IORA provide political dialogue platforms. PERSGA supports environmental protection, while IONS strengthens naval interoperability.

3.7 Reference to Improving the RMSS

During the development of this strategy, some areas for enhancing the draft RMSS were identified. These are set out in the Improving the RMSS annex, which identifies key enhancements: integration of WG3 as an operational anchor, institutionalisation of industry engagement, improved Investment and support partnership, inclusion of cyber and HA/DR, gender mainstreaming, and SMART KPIs. These enhancements are cross-referenced throughout the Engagement Strategy but presented in full as a separate annex for clarity.

4 ACTION PLAN

The Action Plan translates strategic objectives into concrete, measurable activities for DCoC States and partners. It is structured around seven key areas: governance, operational cooperation, legal harmonization, coordination of support, industry engagement, resilience, and gender and inclusion. Each area contains specific actions, deliverables, and KPIs, which are summarised below. Detailed baselines, targets, and responsibilities are provided in Appendix A.

4.1 Governance & National Coordination

States should establish or strengthen National Maritime Security Committees (NMSCs) with clear legal mandates, ensuring inter-ministerial coordination, and develop NMSRRs and national maritime security strategies. Gender and youth representation should be mainstreamed across governance structures. Progress will be measured by the number of fully operational NMSRRs and NMSCs by 2027 (target: 12 States) (RMSS §2.3.2).

4.2 Operational Cooperation

WG3 is the anchor for practical cooperation at sea. States should adopt SOPs for joint patrols, biennial threat assessments, regional vessel databases, ship-rider agreements, SAR, evidence handling, and information routing across the ISN (RMSS §1.1.6; §1.2.2.3). By 2027, at least eight NMISCs should be fully operational, and WG3 should conduct two multinational exercises annually, with industry observers integrated.

4.3 Legal Harmonization & Prosecutions

All signatory States should harmonise national maritime legislation with DCoC/JA provisions (RMSS §2.3.2.1). By 2027, at least 15 States should have adopted harmonised legislation, and a Regional Legal Forum should convene annually to assess prosecutions and promote mutual legal assistance (RMSS §2.3.5).

4.4 Coordination of support & Trust Fund

Donor engagement should be consolidated through an annual donor roundtable aligned with the Capacity Building Matrix (RMSS §2.2.4.4). By 2027, the DCoC Trust Fund should be operational, with contributions from at least three donors and one private-sector consortium (RMSS §2.2.4.7).

4.5 Industry Engagement

A Public–Private Maritime Security Forum should be launched to institutionalise industry reporting, resilience planning, and cyber awareness. By 2026, voluntary industry reporting should be integrated into ISN platforms, with participation from at least 50% of major carriers (RMSS §1.2.2.3).

4.6 Resilience (Cyber, Environmental, Infrastructure)

Resilience in this strategy is understood as the ability of States and the region to withstand and adapt to shocks across multiple domains. This includes not only cyber resilience but also preparedness for humanitarian assistance and disaster response (HA/DR), protection of critical maritime infrastructure, and environmental security in line with PERSGA and IMO frameworks. Linking these dimensions ensures that resilience is not a catch-all concept, but a coherent line of effort that addresses interrelated vulnerabilities in the maritime domain. By 2026, States should adopt a cyber resilience policy framework for ports and MDA systems (RMSS §3.5.1). Regional HA/DR exercises should be conducted annually, addressing oil spills, natural disasters, or mass rescue operations (RMSS §3.4.3.5). By 2028, risk assessments of critical undersea cables and offshore installations should be completed (RMSS §3.1.1.5).

4.7 Gender and Inclusion

Gender and inclusion will be mainstreamed across governance, operations, and capacity-building. Current participation of women and youth in national and regional maritime security structures is estimated at less than 10% based on 2023–2024 national reports and IMO records. The strategy sets a target of at least 30% participation by 2028, aligned with RMSS principles and national strategies on gender equality where available. Progress will be measured annually through NMSCs and WG reporting, ensuring that targets are evidence-based and consistent with wider regional and UN frameworks.

5 NEXT STEPS FOR STATES

The Engagement Strategy concludes with a focused set of immediate next steps for DCoC States. These actions represent practical, achievable priorities that can be initiated within the next 12–24 months to create momentum, demonstrate commitment, and provide a foundation for longer-term consolidation. They are derived from the Action Plan and sequenced to align with RMSS priorities.

Priority Actions

1. Establish or legally mandate National Maritime Security Committees (NMSCs) in all signatory States, ensuring inter-ministerial representation and clear mandates for maritime security coordination (RMSS §2.3.2).
2. Adopt Standard Operating Procedures (SOPs) for information routing across the Information Sharing Network (ISN), enabling secure, interoperable reporting and response (RMSS §1.2.2.3).
3. Accelerate the development of National Maritime Information Sharing Centres (NMISCs), following the Kenya and Tanzania roadmaps, and commit staffing and ICT resources (RMSS §1.1.6).
4. Commit vessels, aircraft, and personnel to WG3-led operations and exercises, including participation in at least two multinational exercises annually (RMSS §2.5.7).
5. Harmonise national legislation with DCoC/JA provisions, supported by the establishment of a Regional Legal Forum to review prosecutions and facilitate mutual legal assistance (RMSS §2.3.2.1; §2.3.5).
6. Launch a Public–Private Maritime Security Forum to institutionalise industry engagement in reporting, cyber resilience, and crisis response planning (RMSS §1.2.2.3; §3.5.1).

Conclusion

Taken together, these steps represent a coherent and achievable near-term agenda. Their implementation will demonstrate political commitment, build operational capacity, and signal to donors and industry that the DCoC is the credible framework for maritime security in the region. Progress should be reviewed annually by the DCoC Steering Committee, with adjustments made in line with evolving threats and opportunities.

APPENDIX A

DCOC ENGAGEMENT STRATEGY – DETAILED ACTION PLAN FOR SIGNATORY STATES

1. Introduction

This Action Plan translates the Djibouti Code of Conduct (DCoC) Engagement Strategy into practical actions for signatory States. It provides measurable Key Performance Indicators (KPIs), directly referenced to the Regional Maritime Security Strategy (RMSS) Ends, Ways, and Means framework.

2. Strategic Objectives (from RMSS)

- Enhance governance and coordination (§2.1.1, §2.3.2).
- Strengthen operational cooperation and the ISN (§1.1.6, §1.2.2.3).
- Harmonise legal frameworks and enable prosecutions (§2.3.2.1).
- Promote Coordination of support and financial sustainability (§2.2.4.4, §2.2.4.7).
- Advance inclusivity, gender, and youth participation (§3.1.1.5).
- Build resilience in cyber, environment, and infrastructure security (§3.4.3.5, §3.5.4).

3. Action Areas & KPIs

A. Governance & National Coordination

- Actions:
 - Establish/strengthen National Maritime Security Committees (NMSCs).
 - Create NMISC Sub-Working Groups (where not already present).
 - Mainstream gender/youth (target 30% participation by 2028).
- KPIs:
 - # of States with functioning NMSCs and Sub-WGs (baseline 2025: 4; target 2027: 12).
 - % female/youth participation in WG activities (baseline 10%; target 30% by 2028).

RMSS Reference: §2.3.2; §3.1.1.5

B. Operational Cooperation (WG3 Roadmap & ISN)

- Actions:
 - Finalise SOPs for patrols, SAR, and evidence handling (by 2026).
 - Support NMISC development (Kenya 24m roadmap; Tanzania 16m roadmap as models).
 - Conduct at least 2 multinational exercises annually with industry observers.
- KPIs:
 - # of States with NMISCs at Initial/Full Operational Capability (baseline 2; target 8 by 2027).
 - # of joint patrol days and SAR operations coordinated via WG3 (baseline 0; target 150 days by 2028).
 - # of WG3-led exercises with industry observers (baseline 0; target 2 annually from 2027).

RMSS Reference: §1.1.6; §1.2.2.3; §2.5.7

C. Legal Harmonisation & Prosecutions

- Actions:
 - Convene Regional Legal Forum under IMO auspices.
 - Align national laws on piracy, trafficking, and cybercrime.
 - Develop regional SOPs for chain-of-custody and legal finish.
- KPIs:
 - # of States with harmonised maritime security legislation (baseline 5; target 15 by 2027).
 - % of maritime crime cases successfully prosecuted regionally (baseline 20%; target 50% by 2028).

RMSS Reference: §2.3.2.1

D. Coordination of support & Resource Mobilization

- Actions:
 - Hold annual Donor & Friends of DCoC Roundtable.
 - Operationalise DCoC Trust Fund with transparent project pipeline.
 - Align donor pledges to CB Matrix gaps.
- KPIs:
 - # of annual donor roundtables held (baseline 0; target 1 annually).

- % of donor-funded projects aligned with CB Matrix (baseline 40%; target 90% by 2027).
- Trust Fund contributions pledged (baseline \$0; target \$25m by 2028).

RMSS Reference: §2.2.4.4; §2.2.4.7

E. Industry Engagement & Voluntary Reporting

- Actions:
 - Launch Public–Private Maritime Security Forum (by 2026).
 - Expand voluntary industry reporting into ISN (target 50% major carriers by 2027).
 - Pilot cyber incident reporting SOPs with ports and shipping lines.
- KPIs:
 - # of industry partners enrolled in voluntary reporting (baseline 0; target 50% carriers by 2027).
 - # of Public–Private Forum meetings held annually (baseline 0; target 2 by 2027).
 - # of cyber incident reports processed via ISN (baseline 0; target 25 by 2027).

RMSS Reference: §1.2.2.3; §3.5.4

F. Resilience (Cyber, Environmental, Critical Infrastructure)

- Actions:
 - Integrate cyber and HA/DR into WG3 training/exercises.
 - Institutionalise annual HA/DR drills by 2027.
 - Conduct regular undersea cable/port risk assessments.
- KPIs:
 - # of States with cyber-SOPs integrated into NMISCs (baseline 0; target 10 by 2027).
 - # of HA/DR exercises held annually (baseline 0; target 1 in 2026; 2 annually from 2027).
 - # of port/undersea cable risk assessments conducted (baseline 0; target 10 by 2028).

RMSS Reference: §3.4.3.5; §3.5.4

G: Gender & Inclusion with activities and KPIs.

- **Actions:**

- Integrate gender/youth representation in all NMSCs and NMISC Sub-Working Groups (target 30% by 2028).
- Ensure training programs and exercises (WG2/WG3) achieve minimum 30% female/youth participation.
- Develop mentorship and scholarship programs for young professionals in maritime security, fisheries, and law enforcement.
- Introduce gender-sensitive SOPs for SAR and detention to protect vulnerable groups.
- Partner with civil society and women's associations to build legitimacy and awareness.

KPIs:

- % of women/youth in governance and WG structures (baseline 10%, target 30% by 2028).
- of trainings/exercises meeting 30% gender/youth participation.
- of gender-sensitive SOPs adopted (target: 3 by 2027).
- of mentorship/scholarship placements for youth (target: 50 by 2028).

RMSS References: §3.1.1.5; §1.4.3.1; §2.3.2

4. Monitoring & Evaluation

Monitoring of this Action Plan will be undertaken through quarterly reporting via the DCoC Engagement Portal, annual Steering Committee reviews of KPIs, biennial RMSS reviews, and an independent evaluation at 5 years.

Appendix A – Detailed Action Plan

Deliverable	KPI	Baseline	Target & Date	Lead Actors	RMSS §
NMSCs & NMISC Sub-WGs legally established	# States with instruments in force	4 (2025)	12 by end-2027	States; IMO (advice)	§2.3.2
ISN Routing & Classification SOP approved	% incident reports present in ISN within 24h	Not measured	≥90% by 2027	WG1/WG3; NMISCs; RMIFC/RCOC	§1.2.2.3
WG3 joint ops/exercise calendar live	% events logged & deconflicted	Fragmented calendars	100% by 2026; 2 cycles/yr	WG3 Secretariat; CMF; EUNAVFOR; States	§2.5.7
IORIS rooms for all NMISCs	# active rooms; # incidents coordinated	0 (2025)	6 rooms; ≥12 incidents by 2027	States; CRIMARIO/IORIS; RMIFC/RCOC	§1.1.6; §1.2.2.3
Regional evidence chain SOP endorsed	# States applying SOP; admissible case files	Varied practice	SOP 2026; +50% admissible files by 2028	WG3 Legal; Prosecutors; IMO/UNODC observers	§2.3.2.1
Public–Private Maritime Security Forum launched	# industry partners; # meetings/year	0	50% carriers by 2027; 2/yr	States; Industry associations; Insurers; IMO	§1.2.2.3
HA/DR & environmental drills with PERSGA/Nairobi	# drills/year; # ports/cables assessed	0	2 drills/yr; 10 ports/cables by 2028	States; WG3; PERSGA; Nairobi Convention; Ports	§3.4.3.5; §3.5.4

Table A1: Detailed Deliverables, KPIs and Responsibilities

Action Area	Key Actions	KPIs (Baseline → Target)	RMSS §
Governance & National Coordination	Establish NMSCs; NMISC Sub-WGs; gender/youth inclusion	States with NMSCs 4→12 (2027); Women/youth 10%→30% (2028)	§2.3.2; §3.1.1.5
Operational Cooperation (WG3/ISN)	Finalise SOPs; WG3 calendar; IORIS rooms; SHADE standing brief	NMISCs at IOC/FOC 2→8 (2027); joint patrol days 0→150 (2028); 2 WG3 exercises/yr	§1.1.6; §1.2.2.3; §2.5.7
Legal Harmonisation & Prosecutions	Regional Legal Forum; regional evidence chain SOP; align laws	States with harmonised laws 5→15 (2027); prosecutions 20%→50% (2028)	§2.3.2.1
Coordination of support & Trust Fund	Annual Donor Roundtable; CB-Matrix gating; Trust Fund pipeline	≥90% projects aligned by 2027; pledges \$25m by 2028	§2.2.4.4; §2.2.4.7
Industry Engagement & Reporting	Public–Private Forum; voluntary reporting; cyber incident pilots	50% carriers enrolled by 2027; ≥25 cyber reports by 2027	§1.2.2.3; §3.5.4
Resilience (Cyber/Env/Infrastructure)	Integrate cyber & HA/DR in WG3; port/cable risk assessments; PERSGA/Nairobi drills	2 HA/DR drills/yr; 10 ports/cables assessed by 2028; 10 States with cyber SOPs by 2027	§3.4.3.5; §3.5.4

Table A2: Summary Actions and KPIs

APPENDIX B

NEXT STEPS FOR DEVELOPMENT PARTNERS

Introduction

While DCoC States retain primacy in implementing this Engagement Strategy, development partners (donors, Friends of DCoC, international organizations, NGOs, and industry associations) play a critical enabling role. This chapter outlines how partners can align their support with DCoC priorities, avoiding duplication and ensuring coherence with the Regional Maritime Security Strategy (RMSS).

Investment and support partnership

Partners should commit to an annual donor roundtable linked to the Capacity Building (CB) Matrix (RMSS §2.2.4.4). By 2027, the DCoC Trust Fund should be operational, with multi-year pledges from at least three donors and one private-sector consortium (RMSS §2.2.4.7). Predictable financing will replace fragmented projects, providing sustainability.

Industry Engagement

Development partners should support the launch of a Public–Private Maritime Security Forum, integrating shipping, port operators, and offshore stakeholders into the security architecture. Voluntary reporting should be embedded into ISN platforms (Mercury, IORIS, RMIFC, RCOC), with industry funding to enhance cyber resilience (RMSS §1.2.2.3; §3.5.1).

Capacity Building & Training

Partners should align capacity building with the WG2 mandate. Gender and youth participation must be mainstreamed, with a target of 30% representation in training and exercises by 2028 (RMSS §1.4.3.1). Secondments, mentoring, and scholarships to NMISCs will reinforce national expertise.

Operational Support

Naval partners should continue deployments but embed liaison officers into WG3 to improve coordination. Technology sharing, including maritime domain awareness systems, drones, and secure communications, should be prioritised (RMSS §1.1.6).

Accountability & Monitoring

Development partners should publish an annual Investment and support partnership report to ensure transparency and avoid duplication. Independent monitoring and evaluation (M&E) frameworks should be funded to track progress against SMART KPIs.

Priority Next Steps for Development Partners

Pledge contributions to the DCoC Trust Fund (RMSS §2.2.4.7).

Join the annual donor roundtable (RMSS §2.2.4.4).

Support NMISC development with technical and financial assistance.

Provide expertise and resources for legal harmonization and prosecutions.

Fund regional cyber resilience and HA/DR exercises (RMSS §3.5.1; §3.4.3.5).

APPENDIX C – IMPROVING THE DRAFT RMSS

This annex consolidates recommendations and derived tasks from the Improving the RMSS paper. It identifies key enhancements required to strengthen alignment between the RMSS and the DCoC Engagement Strategy.

Improving the draft Regional Maritime Security Strategy (RMSS)

Strengthening Derived Tasks for Implementation and Alignment with the DCoC Engagement Strategy

1. Introduction

The Regional Maritime Security Strategy (RMSS) provides the strategic framework for advancing maritime governance, operational cooperation, and resilience in the Western Indian Ocean and Gulf of Aden. While the RMSS establishes clear Ends, Ways, and Means, the practical delivery of its objectives is constrained by gaps in operationalization, stakeholder engagement, and monitoring.

This paper identifies key gaps in the current RMSS, proposes enhancements, and presents a revised set of Derived Tasks that are specific, measurable, achievable, relevant, and time-bound (SMART). It also outlines how these improvements can be advanced through the Djibouti Code of Conduct (DCoC) Engagement Strategy, ensuring coherence between the two instruments.

2. Gap Analysis of the RMSS

2.1. Operationalization (WG3 Missing)

The RMSS does not reflect the establishment of Working Group 3 (WG3) on Operational Cooperation and Coordination at Sea (2025), which now provides the practical mechanism for joint patrols, SAR, and legal finish.

2.2 Industry and Civil–Military Engagement

While Friends of DCoC are noted, industry engagement is not institutionalized. Shipping companies, port operators, and offshore stakeholders remain outside formal RMSS processes.

2.3 Coordination of support / Financing

The RMSS identifies “Means” but lacks a robust mechanism for Investment and support partnership. The Capacity Building Matrix (CB Matrix) and the DCoC Trust Fund are not fully embedded.

2.4 **New & Emerging Threats**

The RMSS remains somewhat piracy-centric. It does not adequately address cyber security, drones, critical infrastructure, or environmental risks (oil spills, HA/DR).

2.5 **Gender and Inclusion**

No provisions exist for mainstreaming gender or youth participation. Gender and youth participation should be mainstreamed across all Working Groups, NMSCs, and training activities, with SMART KPIs for representation, recruitment, and leadership development

2.6 **Monitoring and Evaluation**

The RMSS lacks measurable performance indicators, limiting accountability.

3. **Enhancements to the RMSS**

3.1 Integrate WG3 as the operational anchor, with phased roadmap guiding implementation.

3.2 Institutionalize industry engagement through a Public–Private Maritime Security Forum.

3.3 Strengthen Coordination of support by aligning pledges with CB Matrix and WG3 phases.

3.4 Expand scope to new threats, particularly cyber and environmental resilience.

3.5 Mainstream gender and inclusion across all Working Groups and training activities.

3.6 Introduce SMART KPIs to measure progress and accountability.

3.7 Include provisions on Threat assessment cycle, NMSRR and regional vessel/crime databases.

4. **Revise Derived Tasks**

The following rephrased Derived Tasks ensure greater clarity, alignment with WG3, and measurable outcomes:

4.1 **Information Sharing**

By 2026, integrate voluntary industry reporting into ISN platforms (Mercury, IORIS, RMIFC, RCOC) with participation from at least 50% of major carriers (RMSS §1.2.2.3; WG3 Phase 1–2).

By 2027, establish SOPs for cyber incident reporting across all signatory States (RMSS §3.5.4.1–§3.5.4.3; WG3 Phase 2).

4.2 Capacity Building

By 2026, complete national capacity gap assessments using the CB Matrix and validate through WG2 (RMSS §1.4.4.1; WG2 mandate).

By 2028, ensure that at least 30% of participants in WG training and exercises are women or youth representatives (RMSS §1.4.3.1; cross-cutting inclusion goal).

4.3 Operational Cooperation (WG3)

By 2026, adopt regional SOPs for joint patrols, SAR, and evidence handling (RMSS §1.1.6; WG3 Phase 1).

By 2027, conduct at least two multinational exercises annually under WG3, with industry observers integrated (RMSS §2.5.7; WG3 Phase 2).

By 2028, operationalize a Joint Maritime Task Force under WG3 Phase 3, capable of coordinated patrols across the region (RMSS §2.4.4.1; WG3 Phase 3).

4.4 Legal Frameworks

By 2027, all signatory States to adopt harmonized maritime legislation aligned with DCoC/JA (RMSS §2.3.2.1; WG3 Legal SOPs).

By 2028, convene an annual Regional Legal Forum to assess prosecutions and promote mutual legal assistance (RMSS §2.3.5; WG3 Phase 2).

4.5 Donor Engagement

By 2026, establish an annual donor roundtable to align contributions with CB Matrix and WG3 Roadmap (RMSS §2.2.4.4; WG3 Phase 1).

By 2027, operationalize the DCoC Trust Fund with contributions from at least three donors and one private-sector consortium (RMSS §2.2.4.7; WG3 Phase 2–3).

4.6 Emerging Threats & Resilience

By 2026, develop a cyber resilience policy framework for ports and MDA systems (RMSS §3.5.1; WG3 Phase 1–2).

By 2027, conduct at least one regional HA/DR exercise annually addressing oil spills, natural disasters, or mass rescue (RMSS §3.4.3.5; WG3 Phase 2–3).

By 2028, complete annual risk assessments of critical undersea cables and offshore installations (RMSS §3.1.1.5; WG3 Phase 3–4).

5. Implications for the DCoC Engagement Strategy

5.1 The Engagement Strategy becomes the delivery vehicle for these improved derived tasks. Specifically:

5.2 Political dialogue mechanisms (Steering Committee, International Partners Forum) will mobilize support.

5.3 Industry inclusion (Public–Private Forum) will drive reporting, resilience, and cyber awareness.

5.4 WG3 Roadmap will provide the operational framework.

5.5 Coordination of support will align with CB Matrix and Trust Fund.

5.6 Gender/inclusion will be mainstreamed through WG training and governance structures.

6. Next Steps

6.1 Validate revised Derived Tasks with DCoC Steering Committee.

6.2 Align donor pledges and WG3 implementation with these tasks.

6.3 Embed SMART KPIs in the Engagement Strategy as a follow-on annex.

6.4 Review progress biennially and revise as necessary.

Annex: Mapping of Current vs. Revised Derived Tasks

Derived Task	Action/Output	Lead Actors	Timeline/Priority	RMSS §
Operationalize WG3	Publish joint ops/exercise calendar; embed legal-finish injects	WG3 Secretariat; States	By 2026 (high)	§2.5.7
Adopt ISN SOP	Standardized routing/classification; 24h back-posting	States; NMISCs; WG1	By 2027	§1.2.2.3
Harmonize laws & prosecutions	Model laws; evidence SOP; MLA templates	States; Prosecutors; IMO/UNODC	2026–27	§2.3.2.1
Industry engagement	Public–Private Forum; voluntary reporting; cyber pilots	States; Industry; Insurers	2026–27	§1.2.2.3; §3.5.4
Resilience/HA-DR	PERSGA/Nairobi drills; port/cable risk assessments	States; Ports; Env. agencies	Annual from 2026	§3.4.3.5; §3.5.4

Table B1: RMSS Improvements and Derived Tasks