1 Risk Assessment Methodology

1.1 Introduction

The purpose of assessing risk is to enable project activity in a safe and secure manner. Recognizing primacy of life as the critical concern, all risk assessments are designed to establish an understanding of the dangers posed by malign actors to project affected personnel in the context of the local environment. These risk assessments do not seek to identify risks posed by natural disasters, acts of God or other causes, neither do they seek to understand the risk to property or project activity.

The assessment methodology employed is a "Risk Based" approach in which risk is a function of the likelihood of a threat, the severity of the consequences, and the vulnerability of the project in terms of the effectiveness of existing and proposed risk mitigation measures.

Table 1.1-1: The assessment follows six stages

1	**Identify Critical Assets.** In this case it is the lives and the safety of the Project affected personnel
2	**Identify Threat Scenarios.** Security threats to the project are identified and the principal threat scenarios are described
3	**Threat Likelihood and Impact.** The threat scenarios identified in the previous stage are ranked in a matrix according to their likelihood and impact
4	**Vulnerability Assessment.** The project's vulnerability to each of the identified threat scenarios is assessed and ranked in terms of the effectiveness of the mitigation measures currently in place
5	**Current Risk Exposure.** The Likelihood, Impact and Vulnerability scores are combined to define the current, pre-treatment risk score.
6	**Post Risk Exposure – Incorporating Local SMP risk mitigation measures.** Working off the risk scores identified in step 5, a local SMP is written providing risk mitigation measures for each identified threat scenario. This results in a new vulnerability score for each threat scenario. This revised score is combined with the earlier Likelihood and Impact scores to give a new risk score.

1.2 Step 1 Critical Assets

These are the critical assets against which the likelihood/ impact of, and vulnerability to, a specific threat scenario is measured is divided into three categories as listed below.

- **Category A** – International project workers (a project worker is any individual employed to fulfil project activity and can be from the PIU, IPs, private contractors or government employees)
- **Category B** – Local National project workers
- **Category C** – Local Population

The risk assessment will measure, for each identified threat scenario, the likelihood, impact and vulnerability, for each category of project affected personnel.

1.3 Step 2 Threats and Scenarios and Information

The threat will be identified through a team that is comprised of local security experts, who are native Somali language speakers, which affords them access to all local reporting across news outlets and social media feeds. These team will have networks across the country which combined with intelligence feeds from FGS, UN and the INGO network will provide an unparalleled understanding of the security situation as well. All security incidents received from all sources are stored in the MoCT PIU database. It is from these security incidents and an understanding of malign actors Tactics, Techniques and Procedures (TTPs) that derives the Threat Scenario Lists.

1.4 Step 3 Threat Likelihood and Impact

Likelihood scores are generated for each threat scenario for each category of project affected personnel. The threat scenarios are then analysed in terms of the potential impact to project affected personnel. The Impact scoring system can be seen below;

Impact Score	Impact	Definition
1	VERY LOW	Insignificant Injuries or health effects
2	LOW	Minimal Injuries or health effects
3	MEDIUM	Moderate Injuries or health effects
4	HIGH	Permanent disability and/or multiple hospitalizations, major health effects
5	EXTREME	Fatalities, multiple permanent disabilities or multiple hospitalizations, major health effects

1.5 Step 4; Vulnerability Assessment

The risks is then analysed using the current risk mitigation measures provided by friendly security forces in the local area, for each threat scenario and each category of project affected person, existing mitigation measures are identified and assigned a score according to their ability to deter, detect or defend against the event. The Vulnerability scoring system can be seen below;

Vulnerability Score	Vulnerability	Definition
1	INSIGNIFICANT	Protection measures are complete.
2	MINOR	Protection measures are extensive and mostly effective; the chances of the event occurring are low.
3	MODERATE	Protection measures are moderate and partly effective: it is possible that the event will occur.
4	MAJOR	Protection measures are few or partly effective; event is probable.
5	EXTREME	Protection measures are non-existent or ineffective; event is expected to occur.

By multiplying the likelihood score with the Impact score and the vulnerability score a Risk Score is generated for each threat scenario for each category of worker. Again, these Risk scores are categorized into ‘Risk Levels’, these are;

- STOP (Project Activity),
- Extreme,
- Substantial,
- Partial
- Low.

Local risk assessments are reviewed continuously and as new information is made available.

1.6 Step 5 Risks Exposure

By multiplying the likelihood score with the Impact score and the vulnerability score a Risk Score is generated for each threat scenario for each category of worker. Likelihood, Impact and Vulnerability Scores range from 1-5, therefore the risk score range is from 1-125. Risk scores are categorised into 'Risk Levels', these can be seen below;

Risk Score	Risk Level	Action Required
76-125	Stop project activity	PROJECT ACTIVITY TO BE SUSPENDED UNTIL RISK SCORE REDUCES (This is likely due to the activity of malign actors, implementing further risk mitigation measures will not have a measurable effect on the risk score).
51-75	Extreme	Implement further mitigation measures with highest priority until risk reduced to acceptable level (<15). If risk cannot be reduced, the safety of project affected personnel is in doubt. Limited project activity allowed to continue on a case by case basis and only after sign off for each proposed activity by PIU Project Coordinator.
31-50	Substantial	Project activity can continue with required risk mitigation measures in place. PIU will continuously review the likelihood of threat scenarios and the risk mitigations measures in place including M&E and audits of activity on the ground.
16-30	Partial	Project activity can continue with required risk mitigation measures in place. PIU will regularly review threat likelihood and risk mitigation measures.
1-15	Low	Project Activity can continue, PIU will regularly review threat likelihood.

In each local SRA a risk score and risk level will be generated for each identified threat scenario, for each category of project affected personnel

1.7 Step 6 Post Risk Exposure – Including SMP Risk Mitigation Measures

For all threat scenarios that are detected in any local SRA a suite of risk mitigation measures will be identified specific to that threat scenario.

For each Risk Level **(STOP, Extreme, Substantial, Partial and Low)** a proportionate amount of these risk mitigation measures will be assigned to the threat scenario. Clearly for both STOP and Extreme risk levels the maximum, realistically achievable risk mitigations will be assigned with the aim of reducing the risk score to below 50.

Factoring in the assigned risk mitigation measures the vulnerability score for each threat scenario will be adjusted. This will lead to a revised risk score and potentially revised risk levels, ideally leading to all threat scenarios with a risk score lower than 50 and a risk level of Substantial, Partial or Low.

1.8 Change to Threat Likelihood

The Security situation in Somalia and particularly within the proposed project activity areas is volatile. As the situation evolves the likelihood score of any particular threat scenario may increase or decrease. The local SRA is a dynamic document. If new information becomes available that materially changes the assessment of the likelihood of a particular threat, the likelihood scores will be adjusted and therefore the risk score for a threat scenario will change. If the change in the risk score moves the threat scenario into a different risk level (STOP, Extreme, Substantial, Partial, Low) then the current risk mitigation measures will no longer be proportional and will need to be adjusted.

If a risk level is raised an immediate flash message will be generated by the PIU. It will be sent to all relevant IPs and Security stakeholders within the EA-RDIP and World Bank. The message will clearly articulate which project activities and locations are affected, which threat scenarios have changed, what the new risk level is and what action is to be taken. Action to be taken may include cessation or curtailing of project activity as well as mandated extra mitigation measures to be implemented by IPs. It is very likely that once a risk level is raised that project activity will be suspended, at least in the short term, to allow IPs to rebalance and put in place new risk mitigation measures.

1.9 Process Example – Local Security Risk Assessment[1]

Step 1 Identify Critical Assets

- **Category A** – International project workers (a project worker is any individual employed to fulfil project activity and can be from the PIU, IPs, private contractors or government employees)
- **Category B** – Local National project workers
- **Category C** – Local Population

Step 2 Identify Threats and Scenarios

- Vehicle Born Improvised Explosive Device
- Person Born Improvised Explosive Device
- Improvised Explosive Device
- Complex Attack
- Indirect Fire attack

Step 3 Establish Threat Likelihood and Impact

Likelihood Scores

Threat Scenario	LIKELIHOOD SCORES		
	Category A	Category B	Category C
Vehicle Born Improvised Explosive Device	4	4	3
Person Born Improvised Explosive Device	4	3	2
Improvised Explosive Device	5	4	3
Complex Attack	4	4	2
Indirect Fire attack	3	4	2

Impact Scores

Threat Scenario	IMPACT SCORES		
	Category A	Category B	Category C
Vehicle Born Improvised Explosive Device	5	5	3
Person Born Improvised Explosive Device	5	5	2
Improvised Explosive Device	4	4	3
Complex Attack	5	5	2
Indirect Fire attack	5	5	2

[1] Source* Somalia Crisis Recovery Project Draft Security Risk Assessment Methodology – HRM February 2021

Vulnerability Scores

Threat Scenario	VULNERABILITY SCORES		
	Category A	Category B	Category C
Vehicle Born Improvised Explosive Device	3	4	3
Person Born Improvised Explosive Device	4	5	3
Improvised Explosive Device	4	4	2
Complex Attack	5	4	3
Indirect Fire attack	4	3	4

1.10 Step 5 Current Risk Exposure

Category A - International Project Workers

Threat Scenario	Category A			
	Likelihood	Impact	Vulnerability	Risk Score
Vehicle Born Improvised Explosive Device	4	5	3	60
Person Born Improvised Explosive Device	4	5	4	80
Improvised Explosive Device	5	4	4	80
Complex Attack	4	5	5	100
Indirect Fire attack	3	5	4	60

Category B – Local National project workers

Threat Scenario	Category B			
	Likelihood	Impact	Vulnerability	Risk Score
Vehicle Born Improvised Explosive Device	4	5	4	80
Person Born Improvised Explosive Device	3	5	5	75
Improvised Explosive Device	4	4	4	64
Complex Attack	4	5	4	80
Indirect Fire attack	4	5	3	60

Category C – Local Population

Threat Scenario	Category C			
	Likelihood	Impact	Vulnerability	Risk Score
Vehicle Born Improvised Explosive Device	3	3	3	27
Person Born Improvised Explosive Device	2	2	3	12
Improvised Explosive Device	3	3	2	18
Complex Attack	2	2	3	12
Indirect Fire attack	2	2	4	16

1.11 Step 6 Post Risk Exposure – Including SMP Risk Mitigation Measures

Serial	Threat Scenarios	Current Risk Score			Risk Mitigation Measures	Revised Vulnerability Score		
		CAT A	CAT B	CAT C		Cat A	Cat B	Cat C
1	Vehicle Born Improvised Explosive Device	60	80	27	-Conduct regular security awareness briefings for all staff and contractors. -Provide regular VBIED recognition and awareness training to all staff and contractors. - Jersey Barriers and Tyre Shredders on entrances to compound to ‘hamper’ deter ram raiding. -Where possible there should be adequate standoff between facility perimeter barrier and accommodation / workshops / stores / offices to protect against blast. -Use of deadly force by armed security personnel to neutralise threat on positive identification. - Visual Search of vehicles at entrance using under vehicle search mirrors in purpose-built blast protection search bay. -Pat-down and metal detection wand search of vehicle driver and passengers prior to entry to facility. - Use of Explosive Detection Dogs. -Visitors vehicles to be parked 50 metres distant from facility perimeter. - Vehicle anti-ram ditch constructed around perimeter of facility. -Government buildings and hotels placement of anti-ram bollards to create maximum stand-off. -Installation of blast protection film on facility glass windows. Use of concrete T-walls and Hesco barriers to protect offices and sleeping accommodation. -Procure / construct ballistically protected refuge on facility (Example: (Crewshield Citadel). -Use of Siren / Air Horn warning signals to alert facility personnel to shelter in refuge with ballistic protection (Crewshield Citadel) -Provide on-site trauma medical packs.	2	3	3
2	Person Born Improvised Explosive Device	80	75	12	Conduct regular security awareness briefings for all staff and contractors. -Conduct vetting / background checks of host nation employees. -PBIED profiling / recognition training for staff and security personnel. -Where possible there should be adequate standoff between facility perimeter barrier and accommodation / workshops / stores / offices to protect against blast. -Use of explosive detection dogs. -X-ray of hand baggage, back packs etc.	3	4	3

					-Ballistically protected search / screening area located with suitable standoff at entrance. -Pat-down and metal detection wand search of all personnel prior to entry to facility. - Visual Search of vehicles for explosive / bomb making material at entrance using under vehicle search mirrors in purpose-built blast protection search bay. -Use of deadly force by armed security personnel if PBIED bomber positively identified. -24 / 7 surveillance of facility perimeter to prevent clandestine entry of explosive material / explosive vest for use by hostile insider. -Random perimeter patrols to prevent clandestine entry of explosive material / explosive vest for use by hostile insider. Procure / construct ballistically protected refuge on facility (Example: (Crewshield Citadel). -Use of Siren / Air Horn warning signals to alert facility personnel to shelter in refuge with ballistic protection. (Crewshield Citadel) - Installation of blast protection film on glass windows. -Provide on-site trauma medical packs. -Use of concrete T-walls and Hesco barriers to protect offices and sleeping accommodation. -Consider deploying covert hostile surveillance detection personnel to monitor activity on the outer perimeter of the facility. (Attacks will normally be preceded by surveillance)			
	Improvised Explosive Device	80	64	18	-Conduct regular security awareness briefings for all staff and contractors. -Provide regular IED recognition and awareness training to all project personnel. -Where possible there should be adequate standoff between facility perimeter barrier and accommodation / workshops / stores / offices to protect against blast. - Visual Search of vehicles for explosive / bomb making material at entrance using under vehicle search mirrors in purpose-built blast protection search bay. - Use of Explosive Detection Dogs. -Installation of blast protection film on facility glass windows. -Use of concrete T-walls and Hesco barriers to protect offices and sleeping accommodation. -SOPs covering actions on IED Incident. -Procure / construct ballistically protected refuge on facility (Example: (Crewshield Citadel). -Use of Siren / Air Horn warning signals to alert facility personnel to shelter in refuge with ballistic protection (Crewshield Citadel).	3	3	2

		🟥	🟧	🟩	-Provide on-site trauma medical packs. -X-ray of hand baggage, back packs etc. -Pat-down and metal detection wand search of all personnel. -24 / 7 surveillance of facility perimeter to prevent clandestine entry of explosive / bomb making material for use by hostile insider. -Random perimeter patrols to prevent clandestine entry of explosive / bomb making material for use by hostile insider. -Conduct vetting / background checks of host nation employees. -SOPs covering actions on IED discovery or detonation. -Facility / site evacuation plan. -Access control policy and procedures. -Issue Project ID Cards to staff and host nation labour employed on site.			
	Complex Attack	100	80	12	Host nation local community warning / proactive intelligence. -Host nation security force intelligence. -Host nation employee intelligence. Crisis management / Incident response plan. -Activate crisis management / incident response teams. -Consider use of host nation army, police, armed PSC guards for the protection of the facility. -Consider deploying covert hostile surveillance detection personnel to monitor activity on the outer perimeter of the facility. (Attacks will normally be preceded by surveillance). -SOPs covering actions on complex attack. - Jersey Barriers and Tyre Shredders on entrances to compound to 'hamper' deter ram raiding. Where possible there should be adequate standoff between facility perimeter barrier and accommodation workshops / stores / offices to protect against blast. - Vehicle anti-ram ditch constructed around perimeter of facility. -Installation of blast protection film on facility glass windows. Use of concrete T-walls and Hesco barriers to protect offices and sleeping accommodation. -Procure / construct ballistically protected refuge on facility (Example: (Crewshield Citadel). -Use of Siren / Air Horn warning signals to alert facility personnel to shelter in refuge with ballistic protection (Crewshield Citadel). -All personnel to don ballistic helmet, ballistic vest with plates, and ballistic eye protection on sounding of alarm. -Ensure adequate supply of serviceable fire suppression equipment on facility. -Provide on-site trauma medical packs. -Use of deadly force by armed security personnel to defend the facility and halt the attack.	4	3	3

		🟥	🟥	🟩	-Conduct regular response plan rehearsals (where possible involve host nation security forces). -Only hotels surveyed and approved by project security to be utilized by project staff. -Access control policy and procedures. -Issue Project ID Cards to staff and host nation labour employed on site. -Facility / site evacuation plan. -Incident reporting procedure. -Medevac plan -Ensure that facility is not located close to military / police posts or government offices that could be attractive targets for terrorist / insurgent attacks.			
	Indirect Fire attack	60	60	16	- Host nation local community warning / proactive intelligence. -Host nation security force intelligence. -Host nation employee intelligence. -Crisis management / Incident response plan. -Activate crisis management / incident response teams. -Conduct regular security awareness briefings for all staff and contractors. -Installation of blast protection film on facility glass windows. Use of concrete T-walls and Hesco barriers to protect offices and sleeping accommodation. -Consider deployment of Hesco Ancillary Lightweight Overhead Protective System (LOPS) -Construct adequate number of 'Duck and Cover' shelters with overhead protection sufficiently robust to mitigate prevailing indirect fire threat. -Develop SOPs and a contingency plan for Indirect Fire Attack. -Provide on-site trauma medical packs. -Use of Siren / Air Horn warning signals to alert facility personnel to shelter in refuge with ballistic protection. -All personnel to don ballistic helmet, ballistic vest with plates, and ballistic eye protection on sounding of alarm. -Facility / site evacuation plan. -Incident reporting procedure. -Access control policy and procedures. -Issue Project ID Cards to staff and host nation labour employed on facility /site. (Mitigate ability of hostile element to infiltrate facility /site and identify targets). Medevac plan. -Ensure that facility is not located close to military / police posts or government offices that could be attractive targets for terrorist / insurgent attacks.	3	2	3

1.12 Post Treatment Risk Score Card

Threat Scenario	Pre Treatment Risk		
	Category A	Category B	Category C
Vehicle Born Improvised Explosive Device	60	80	27
Person Born Improvised Explosive Device	80	75	12
Improvised Explosive Device	80	64	18
Complex Attack	100	80	12
Indirect Fire attack	60	60	16

1.13 Post Treatment Risk Score Card

Threat Scenario	Post Treatment Risk		
	Category A	Category B	Category C
Vehicle Born Improvised Explosive Device	40	60	27
Person Born Improvised Explosive Device	60	60	12
Improvised Explosive Device	60	48	18
Complex Attack	60	60	12
Indirect Fire attack	40	45	16