[Draft version]

[Under development]

**SECURITY RISK MANAGEMENT PROCESS**

The safety and security of personnel has become an underlying element of all operations for all organizations. Security must be part of all planning and programming processes and the security cost of doing business must be reflected in all budgets.

In this regard, Security Risk Management methodology becomes of great importance. Risk management does not represent an end itself but is a tool to enable operations. Security Risk Management comprises two main phases: threat and risk assessment and risk mitigation and implementation.

This brief provides a high level summary of the SRM methodology and how to link it with programming/planning operations.

A) Threat and Risk Assessment encompasses:

* Assessing the operations concept, mission and programme;
* Understanding the context of the operation (political, socio-economic, security, environmental, natural);
* Identifying the threats per operation/mission component, which comprises:
  1. Listing, qualifying and quantifying the threats (political, socio-economic, security, natural, etc.)
  2. Understanding the causes of the threat; causes could be addressed through programs/projects;
  3. Being aware of own vulnerabilities and weaknesses, but also strengths;
* Assessing the risk per mission and the operation component, which comprises:

1. Analyzing the possible impact and the consequence the threats may have on the operation;

2. Evaluating the likelihood of the threat materializing and impacting programmes/projects operations;

3. Assigning risk level;

4. Comparing the risk with an approved risk matrix;

6. Taking risk decision;

5. Managing the risk (transferring, mitigating, accepting, avoiding risk);

B) Risk mitigation consists of:

* Developing Risk mitigation measures for threats, causes, weaknesses/strengths, impact and probability;
* Assessing residual risk after mitigation measures are implemented (comparing the risk level with the risk level matrix);
* Making a Risk Decision (avoiding, accepting, transferring and rejecting);
* Implementing the mitigation measures through:

1. The development of operational and mitigation options, and the selection of the best risk option

2. The implementation of the security plan;

3. The resources

4. The accountabilities/mandates for the policy decisions

5. The communication of the plan;

* Monitoring, reviewing and correcting the action.

**INTEGRATING SECURITY RISK MANAGEMENT AND PROGRAMMING CYCLE**



**SAMPLE OF SECURITY MANGEMENT WORK SHEET**

**Per project/ per component**:



**Risk level: \_\_\_\_\_\_\_\_\_ Risk decision: \_\_\_\_\_\_\_\_\_ Accepted / Rework**

**SAMPLE OF SECURITY RISK MANAGEMENT MATRIX**



**E = Extreme H = High M = Medium L = Low N = Negligible**

**Ideally risk should be Low or Negligible**

**TERMINOLOGY**

**Risk:** Risk results from the probability multiplied by impact of a treat interacting on staff, assets, and mission.

**Threat:** Any condition causing death/injury, damage or loss to staff, property, mission (political, security, socio-economic, natural/terrain).

**Vulnerability:** weakness, deficiencies, failures (training, equipment, mindset, procedures, structural, government capacities).