SECURTIY RISK MANAGEMENT

NGO APPROACH

InterAction Security Unit

SUPPORTING MATERIAL
  Graphics

INTRODUCTION

In 1991, InterAction created the Security Advisory Group (SAG). The intent of the SAG was to develop training modules for NGOs operating in austere environments. The result is the basic security training that is currently provided by the London based NGO Red R.

Overall responsibility for the safety and security of NGO staff rests with the host government. However, accountability rests with managers at *all levels*, not only with their security focal points. Security focal points must provide the technical security inputs and advice that allows management officials to make informed decisions for managing security risks. Security risk management therefore requires good teamwork between those who plan and direct NGO operations and those who advise on the security measures which enable them.

These instructions better describe the SRM process, provide enhanced descriptions, updated definitions, procedures and incorporate lessons learned and best practices developed by security officers in the field and at headquarters and in cooperation with the InterAction Security Unit, the InterAction SAG, and the UNDSS through Saving Lives Together. This effort clarifies definitions, makes the current processes easy to understand and share, and provides detailed instructions on preparing critical components of the Security Risk Assessment (SRA).

We encourage you to send your ideas and feedback to continue improving this instruction to jschafer@interaction.org

SCOPE

This document describes the SRM process recommended by the SAG and provides instructions for its use.

This document serves as the guideline for the preparation and use of the Security Risk Assessment (SRA) which is a critical component of the Security Risk Management (SRM) process.

The main focus is on the 'Preparation' phase of the process, which provides the user with tools to identify and assess the NGO's operational context (activities and the security realities), evaluate the problem (risk analysis), and identify solutions (Mitigation Measures) to accomplish its mission of enabling operations while ensuring the safety and security of NGO personnel, assets, and programs.

It is important to note the SRM process does not seek to inhibit current practices or the use of other security management tools by security focal points and decision makers. Rather, it provides a logical and standardized means to ensure all facets of threat and risk are identified and incorporated into each aspect of NGO planning.

Use of a standardized process facilitates the work of the individual NGO and management with security responsibilities in supporting field requirements for additional security resources, in order to effectively undertake its activities. Additionally, the process is unique for each organization and benefits the entire NGO community.

Security is a vital responsibility of all NGO personnel; while absolute security can never be guaranteed, threats and their associated risks can be mitigated and vulnerabilities reduced once identified and assessed. A formalized security risk management process is the key to accomplishing this vital function.

The SRM process outlined in this document is a practical process by which the complex issues surrounding security can be identified and assessed so as to arrive at comprehensive and focused mitigation measures. The process, which is based on modern security risk management practices, will also produce solid rationale for the necessary expenditures on physical security measures, equipment, services, or other security-related requirements.

Circumstances bearing on security continuously change. For this reason, the SRM process should become an integral part of security management. In this manner, all concerned can be assured of up to date, relevant, comprehensive, and cost-effective security planning.

Introduction

The purpose of this section is to explain the SRM and SRA process and clarify the responsibilities of those involved in the preparation and review of SRAs. In order to do this, however, it is necessary to outline those activities of the wider SRM process which connect with the stages of the SRA.

Key terminology

Threat and *Risk* are defined as follows:

> <u>Threat</u>: Any factors (actions, circumstances, or events) which have the potential or possibility to cause harm, loss, or damage to the NGO, including its personnel, assets, and operations.

> <u>Risk</u>: The combination of the *impact* and *likelihood* for harm, loss, or damage to NGOs from the exposure to threats. Risks are categorized in levels from Very Low to Very High for their prioritization.

Security Management Team (SMT) is defined as follows:

> The team that consists of the persons in charge of the NGO country program, finance, logistics, security focal points, top level management (possible second), and national staff representation. The intent of the team is to approve the SRA, and take responsibility for and implement the mitigation of the threats while enhancing the safety and security of the staff, assets, and activities of that particular NGO.

Security Risk Management (SRM)

The Security Risk Management model is the managerial tool of NGOs for the analysis of safety and security hazards that may affect its personnel, assets and operations.

The definition of *Security Risk Management* is:

> SRM is an analytical procedure that assists in assessing the *operational context of the NGO*; and *identifies the <u>risk level</u>* of undesirable events that may affect <u>personnel</u>, <u>assets</u>, and <u>operations</u>; providing guidance on the implementation of *solutions* in the form of specific <u>mitigation</u> strategies and measures with the aim of lowering the risk levels for the NGO by reducing the <u>impact</u> and <u>likelihood</u> of an undesirable event.

Security Risk Assessment (SRA)

The Security Risk Assessment (SRA) is an integral part of the SRM process. Security decisions, planning, and implementation of security measures to manage security risks must be based on sound Security Risk Assessments.

The definition of *Security Risk Assessment* is:

> The process of identifying those threats which could affect personnel, assets or operations and the NGOs vulnerability to them, assessing risks to the NGO in terms of likelihood and impact, prioritizing those risks and identifying mitigations strategies and measures.

A credible SRA is an essential prerequisite to the effective management of risk; the objective of an SRA is to identify and assess the nature of the risks to a NGO operation or activity so that those risks can be effectively *managed* and funded through the application of mitigating measures. (The functioning of the SRA within the overall SRM process is illustrated in Graph 1.)

The Security Risk Management (SRM) Model:

Preparation Phase (Security Risk Assessment-SRA)

The "Realities"

The "Problems"

The "Solutions"

Execution Phase

Programme Assessment

| Location | Activity |

Threat Assessment

| Specific Threats | Situation |

Vulnerability Assessment

| NGO Strengths | NGO Weaknesses |

| Impact | Likelihood |

Risk Analysis

Risk Level (current)

Adjust Activity

Change Location

Reduce Weaknesses

Increase Strengths

Control/Mitigation Measures

| Avoid | Transfer | Reduce Likelihood | Reduce Impact |

| Wrong Place Wrong Time | Risk Level (residual) |

Decision Making

| Risk Acceptability Mitigation Procedures | Establish Priorities | | | Approval of Funding and Resources |
| | Image and Strategy | Time Frame | Cost of Control | |

Prepare and Implement Control Measures

| Security Policies and Procedures | Contingency Plans |

Review and Update

Graph 1 – The Security Risk Management model

Frequency of Completing and Updating Security Risk Assessments

The Security Risk Assessment tool is a living document which must be under constant review. In particular, a validation should be carried out when there is a change or development in the "Security Situation" (PA, TA or VA) which could affect NGO operations or activities. For example:

a. There is a change in the political situation or an upcoming event of political significance (e.g. an election) that may impact on security.
b. There is a change in the operational context (i.e. new role for the NGO or elements of the NGO in country).
c. Or when planning for:
    i. A new mission to be deployed.
    ii. The consideration and selection of new offices or facilities.
    iii. An expansion of programs into new areas of a country.
    iv. Operations resuming after a program suspension, relocation or evacuation for security reasons.
    v. Special events or conferences.
    vi. New spending on security measures.

If new information is reported that changes the SRA, it should be noted to the SMT, addressed in the SMT minutes, and agreed by all members. The SRA matrix should then be updated to contain the relevant changes, conclusions, and new recommendations which were decided in the SMT.

Security Risk Analysis Table

The InterAction SAG established the following table for the evaluation of "Risks Levels" and recommended usage by InterAction members in the spring 2007 SAG meeting. In this process, the impact and likelihood of each specific threat (identified in the previous stages) is processed trough the table resulting in the selection of the corresponding current risk level.

RISK ANALYSIS TABLE		IMPACT				
		Negligible	Minor	Moderate	Severe	Critical
L I K E L I H O O D	Very Likely	Low	Medium	High	Very High	Very High
	Likely	Low	Medium	High	High	Very High
	Moderately Likely	Very Low	Low	Medium	High	High
	Unlikely	Very Low	Low	Low	Medium	Medium
	Very Unlikely	Very Low	Very Low	Very Low	Low	Low

Graph 2 – Risk Analysis Table

Risk Acceptability

For risk levels identified as Medium, High, or Very High, "acceptable risk" is a relative term which requires judgment, not just the application of rules. **The determination of "acceptable risk" is a critical responsibility of senior managers**. The relationship between Program Criticality and the risk to the safety and security of personnel must be considered in the determination of "acceptable risk." Managers must constantly strive to balance these two critical functions in order to create and mange a "culture of security."

In determining the threshold for "acceptable risk" in any given situation one must consider the following questions:

1. Would the consequences of not implementing the program be so serious that the NGO is prepared to accept a "HIGH" or "VERY HIGH" risk to staff lives (as assessed in the SRA)?
2. Has everything possible been done to find alternative methods of achieving the program objectives?
3. Has every possible security measure including the transfer of resources at the expense of other programs been applied to mitigate the security risks so as to reduce the "current risk level" to "MEDIUM" or lower?
4. Is there an adequate system to manage the residual risk in order to ensure that it does not increase beyond the current level?

Only if the answer to all of the above questions is "yes" should the program be implemented.

Finalization of SRAs (*This process varies upon organization*)

The process for finalization of the SRA has some salient steps; they are:

a. The SFP (Security Focal Point) submits draft SRA to the SMT and copies the regional director.
b. The regional director informally reviews the draft SRA and provides the SFP with advice on the following:
    i. With format and process.
    ii. Consistency with recent history of the region/country.
    iii. Actions and decisions adopted in respect to any risk identified as High or Very High
c. SMT approves the SRA in the SMT minutes, which will include and explain any reservations or minority opinions
d. The regional director endorses and returns the SRA.

INSTRUCTIONS

SRM is a process that assists in assessing the *operational context of NGOs* and *evaluates the <u>risk level</u>* of undesirable events that may affect <u>personnel</u>, <u>assets,</u> and <u>operations</u>. It provides guidance on the implementation of *solutions* in the form of specific <u>mitigation</u> measures, targeted at lowering the risk levels by reducing the <u>impact</u> and <u>likelihood</u> of an undesirable event.

The SRM process enables a standardized and flexible approach to the conduct and articulation of a SRA, which is a practical tool that can be utilized for deep field, country, and headquarter locations. It should be prepared by trained security personnel in cooperation with the appropriate country and HQ management structures to address key security focal points.

The continuous review of the SRA enables timely and systematic reviews of Security Phases and other security-related decisions and recommendations. Almost all decisions of the SMT should be supported by an SRA.

In the **Preparation** phase:
- Each of the <u>Program</u>, <u>Threat</u>, and <u>Vulnerability</u> <u>Assessments</u> incorporates the collection of information from the situation and deduction of relevant facts, and provides the essential data required to determine risk.
- During <u>Risk Analysis</u>, determining risk levels for each specific threat scenario is made based on the deductions provided from the three assessments.
- In the <u>Mitigation Measures</u>, all available actions are analysed and incorporated for its presentation to decision-makers. All measures presented must be logical, feasible and relevant. While certain standard lists of mitigating measures exist, creativity, and thinking outside the box are very useful techniques that should also be employed.

In the **Execution** phase:
- <u>Decision</u>.
- <u>Implementation</u> of the selected options. Often overlooked, this phase is critical in achieving reduction in the identified risk level. The SRM process does not end with its preparation. The country director, the SMT and all Security Focal Points must ensure that recommendations are approved, budgeted, and implemented. Accountability does not end with the analyses; it ends with personnel, assets, and operations conducted safely both at field and headquarters.
- <u>Review and Update</u> of the SRA.

PREPARATION PHASE

<u>Time and Place:</u>
The "when and where" is an essential element of all security risk assessments. When assessing the operational context (Program, Threat, and Vulnerability Assessments), clear timeframes and geographical locations must be established to set the context in which these are made. Also, NGO operations are directly linked to these two factors.
- The SMT, program management, HQ, and security focal points are most often responsible for the safety and security of NGO operations, assets, and personnel within a geographical area and for the duration of their tour of duty.
- All NGO activities will occur for a certain time in a certain area.
- Threats are also expected to happen in certain places and within a certain timeframe.
- Phases of security are most often implemented by geographical area and revised and updated on specific dates.

The quick delineation of locations and timeframes will be extremely helpful in the conduct of the Risk Analysis, providing a set of common elements to integrate the three assessments and define risk levels for each specific threat. Thus, each assessment and concomitant risk analysis must begin with clear definitions of the locations and the timeframes being assessed.

Examples of the importance of clearly setting time and place in the SRA: The same threat will result in different risk levels depending on when and where it is manifest. A Vehicle Born Improvised Explosive Device (VBIED) attack against a NGO house which has been fully protected by blast walls, film, and other mitigation will have a lower risk level than the same attack against another NGO facility in the same city that has not protected itself against such a threat. Furthermore, the same threat will have a higher risk level if the attack happens during working hours rather than a weekend as it may produce more casualties, and thus be a better option for attackers.

Using as a starting point your assigned area of responsibility, in coordination and cooperation with other NGOs, the UN, the host government, and all actors relevant to safety and security issues, obtain the information required for the SRA.

Before initiating the Assessments, organize your Country/Area/Duty Station:
- Identify the different regions in your area of responsibility
  - o Using regional and area of operation maps, identify and organize your area of responsibility.
  - o Start by identifying the different geographical, cultural, ethnic, political, and economical regions.
  - o Make a summary of specific conditions and, as much as possible, associate by area/region.
- Divide your Area of Responsibility in typical security regions
  - o Identify, and mark on a map, the current safety and security conditions based on NGO, UN, and open sources information available (i.e. current UN security phases are often readily available and can assist in this process).
- Decide on an initial Country/Area/Duty Station organization
  - o On the basis of the information collected, prepare a subdivision of your country. Typically it will include at least:
    - ▪ Capital city
    - ▪ Current main security areas (i.e. Phase 1 areas, Phase 2 Areas, etc)
  - o Use the resulting index of areas as the guide for the preparation of the Program, Threat, and Vulnerability Assessments of the SRA.

IMPORTANT NOTE:
The SRA is an interactive process, not a sequential one; when conducting an SRA continually check back to see how newly identified factors might affect previously considered aspects.

ASSESSMENT OF THE OPERATIONAL CONTEXT

Assessments:
The three 'assessments' may be considered in any order, however it is recommended to consider Program Assessment first. In doing so, many other factors from the other assessments will become clear. The focus of the Assessments must be geared toward the interaction of Programs, Threats, and Vulnerabilities.

Program Assessment (PA)

A *program* is normally an activity conducted by an NGO within a certain time frame and location.

The Program Assessment is essential to the SRA. It is a distinct and separate part of the process, which is fundamental to planning. The Program Assessment must be developed as a collaborative effort between the responsible country directors, program directors, and national staff members (usually the program officers) who will conduct the programs and security, advisers (including security officers where present) in order to ensure "mainstreaming" of security at the earliest stage of Country/Area Program Operations Planning. It is critical that security focal points are consulted early in all activity assessments prior to grant submission or program development to ensure that threat mitigation decisions are identified and included in grant proposals for proper funding of security training, insurance coverage, emergency equipment, and administration to avoid delays in programs implementation.

The Program Assessment should identify all of the NGO's operations that may be affected by threats. It should assess how and why particular threats could affect programs and also identify those threats, which although present, are less likely to affect the NGO or may be irrelevant to the NGO's operations. A comprehensive picture of program activities should be constructed to allow integration with security information.

The Program Assessment should also contain the assessment of the "criticality" of the program. "Program criticality" defines:

1. The negative consequences (political, humanitarian, economic, security) of not implementing the program or cancelling an existing program.
2. The extent to which other NGO activities/programs are dependent on the program's continued implementation.

For security assessment purposes it may also be described as activities in a certain area or facility. Thus, for its use in the SRM, the *Program Assessment* is an identification, localization, and evaluation of implementation methodology of NGO activities in a given environment.
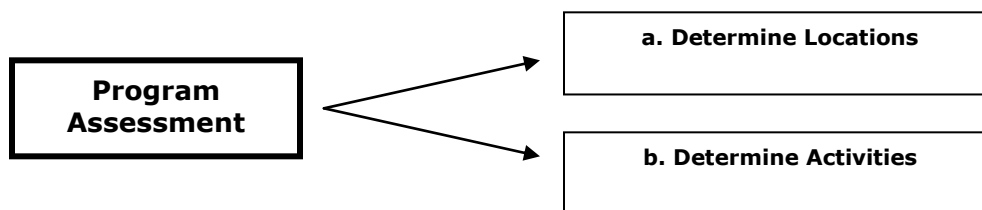
Graph 3 – Steps within the Program Assessment (PA)

Locations: The *Program Assessment* must start with the grouping of all programs and activities within specific geographical locations providing the 'where' for the assessment. In the previous step you have organized your AoR (Area of Responsibility). This provided you with the **"Where"** for the Program Assessment.

Activities: For each location, the Security officer will obtain 'operational' information on NGO <u>activities</u>. This will respond the basic questions of: what, when, who, why, and how.

Identify and locate the NGO team: Who is there? (Or who will be?)

The information gathering process must be geared toward providing responses to the basic questions of who, what, where, when, how, and why. The information gathered must allow the security officer to identify *how, when, and where* NGO personnel are going to work, live, and move—the *criticality, relevance, urgency, needs, and methods* of each NGO operation. It also identifies *how, when, and where* NGO Assets going to be deployed.

To facilitate the collection and analysis, it is best to group the information:
<u>Current operations</u> (currently in progress and budgeted):
    NGO operations and activities;
    NGO personnel deployment;
    NGO facilities and installations.
<u>Planned operations:</u>
    Medium term (to initiate in less than one year; budget already approved or about to be);
    Long term (will start in more than one year; budget being processed).

Example of sound program assessment:
NGO house hosting XX agencies comprising XXX personnel is located in an area subjected to multiple terrorist attacks within last XX months; or, Program X runs humanitarian convoys in Area A that has been affected by multiple incidents of banditry and criminality.


Relevant data should be collected then tabulated for reference during subsequent stages.

Tip:
Security professional must "enable" the safest and most efficient conduct of the programs and activities of the NGO. To successfully accomplish his/her responsibility, security focal points must contact (personally whenever possible) all NGO personnel in his/her area of responsibility and establish an effective network of NGO personnel with security responsibilities at all levels.

Threat Assessment (TA)

Threat Assessments do not provide an assessment of risk, but provide the information and deductions that are used within a Risk Analysis. It consists of two steps: <u>Situational Analysis</u> and determination of <u>General and Specific Threats</u> to NGOs in the area of operations.
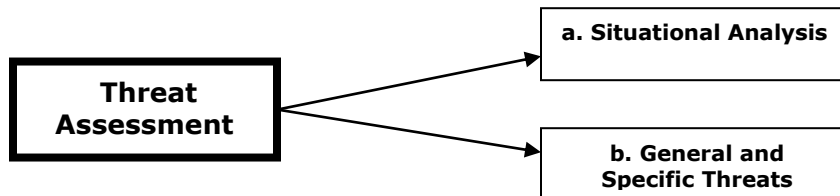
Graph 4 – <u>Steps within the Threat Assessment (TA)</u>

Using the previously established organization of your area of responsibility, identify and assess the country/area safety and security situation.

Situational analysis

The assessment should be relevant to the situation of the NGO locally and should therefore avoid diversions on factors which have no implications for NGO safety and security. This step is the part of the process that supports and allows the identification of general and specific threats to the NGO operation. All data collected must be relevant to safety and security of the activities which the NGO is conducting, supported as much as possible by facts and relevant deductions, and up to date.

- Specific reasons for the inclusion of each threat identified should be outlined either on the basis of trends of security incidents and/or assumptions made.
- Specific reasons as to why identified threats are relevant to the NGO should be outlined.
- Information that is deemed to be important for the determination of threats must be formally registered and filed.

Examples of sound description of security situation:
Multiple terrorist attacks against government facilities using VBIED were executed in 2007; although these did not target the UN or NGOs to date, the perpetrators issued specific warnings to the NGO, and similar attacks on NGO and UN related facilities cannot be ruled out;
In the last reporting period there were multiple robberies of foreign tourists in area A, thus personnel can be affected by similar crimes in this area.

Not all information collected will necessarily be relevant to security risk management. Throughout each step of the security risk management process, information being examined should be filtered by asking the question "*Is this piece of information relevant to our security*?"

This technique will assist in managing the volume of information being considered within the SRM process. It will also lead to a list of required actions to be addressed in the security plan.

General Threats and Specific Threat Scenarios

General Threats: Extracting the relevant information from the previous step, identify, define, and list the general threats to NGOs (i.e. terrorist attack, crime, military conflicts, post-conflict environment, etc.). These threats should be further delineated on the basis of evidence and/or assumptions, thus evolving into detailed *specific threats[1],* i.e. terrorism – in what form: IED, VBIED, suicidal, small arms? Crime—burglary, robbery, sexual assault, carjacking? Military conflicts—cross fire, targeted attacks, access restrictions? Post-conflict threats—land mines, UXO, destroyed infrastructure, roads and bridges?

Programs of the NGO that can be affected by threats identified should be clearly defined, such as NGO offices and facilities, personnel at residence, vehicles, or commuting personnel.

In support of your assessment always seek information and facts on the "HIC" of each threat (History – Intention – Capabilities).

HIC		
History	**Intention**	**Capabilities**
Historic interest	Current interest	Access to region
Historic attacks	Current surveillance	Material resources
Current interest	Documented threats	Technical skills
Current surveillance		Planning /organizational skills
Documented threats		Financial resources

---

[1] Specific threat: Threat that result from the analysis of the general threats previously identified. It's a concise description of an individual threat whose resulting risk level can be mitigated by the NGO. It must be written as a very brief scenario and include: location; methodology; and the minimum technical information required to support the risk analysis (what/how and when/where)

<u>Specific Threat Scenarios</u>: For each general threat, identify and develop their resulting specific threat scenarios. Each specific threat scenario must respond to questions of: what, how, where, and when.

Examples correctly identifying threats to the NGO:
Direct threat of terrorist attack (what) *on NGO offices* (where) *with/by VBIED, individual intruders, fire arms,* (how) *in the next 3 months* (when);
Direct threat of criminal assault (what) *anywhere in the city of ...* (where) *against NGO personnel by car jacking* (how), *at any moment particularly late in the night* (when).

Identified threats should be qualified as direct or indirect/collateral (i.e. collateral threats to NGO personnel from terrorist attacks at public places, or, direct threats of terrorist attacks on NGO offices, or residual crime against NGO personnel in public places, etc.). A threat may fit into more than one category (i.e. perceived and direct).

To provide further details on their individual importance, specific threats may also be categorized into four general types:

- 'Perceived' threats – possible but no clear information (i.e. a threatening telephone call without known substance);
- 'Actual' threats – from known criminals, disgruntled individuals, weapon systems, prior attacks;
- 'Direct' threats – those directed specifically at the NGOs, similar to the Baghdad bomb attack on the UN on 19 August 2003;
- 'Indirect' threats – that may affect the NGO (i.e. being caught in the wrong place at the wrong time).

IMPORTANT NOTE:
A clear determination of specific threat scenarios is critical to the accurate
identification of effective mitigating measures.
Tip:
Indicators: Prepare a <u>list of "if" and "what if" questions</u> to produce indicators on important trends and changes in the threats that may have a relevant effect on the Risk levels. Make the search for the responses to these questions one of the main priorities of your security team.

Vulnerability Assessment (VA)

This stage identifies the <u>strengths</u> and <u>weaknesses</u> of the NGO's security arrangements in the environment in which the organization conducts its activities. It consists of two steps:

- Determination of NGO strengths;
- Determination of NGO weaknesses.
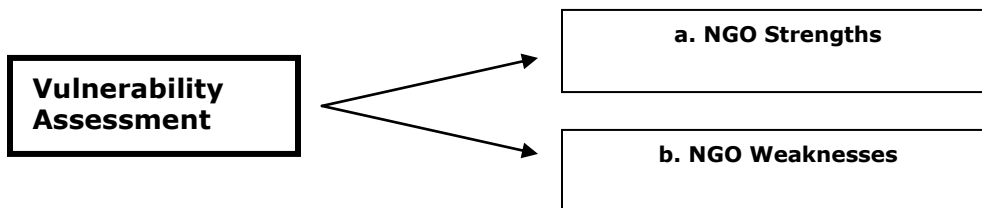
Graph 5 – <u>Steps within the Vulnerability Assessment (VA)</u>

The factors taken into account for this stage are all <u>internal to NGO activities</u> and include as a minimum:

- Location of personnel and assets;
- Exposure of personnel and assets;
- Value of assets;
- Personnel interpersonal skills;
- Security measures in place;
- Degree of compliance with security measures;
- Impact of programs;
- Image of personnel and programs;
- NGO Strengths.

<u>Determination of NGO Strengths:</u> NGO strengths are all factors, including mitigation measures already set in place, that may <u>lessen</u> the impact or likelihood of a threat against the organization.

Examples may include:

well located and protected housing locations, body armour available to personnel, good SOPs, convoy operations for some missions, comprehensive communications network, and implementation of the Security Plan.

Strengths are compared against the NGO weaknesses and will include the security phase, as this is a regulatory system that has significant behavioural and cognitive affects on personnel.

<u>Determination of NGO Weaknesses:</u> These comprise our exposure to the threat. Therefore, our weaknesses are the *gaps/vulnerabilities in current security arrangements,* and any other factor within the activities of the NGO that may <u>enhance</u> the impact or likelihood of a threat against the NGO.

Examples may include:

poor perimeter fencing of compounds, ineffective guard services, lack of support and protection from an uncooperative or incapable host government, missions only able to be conducted by road, a lack of personnel security training, a lack of reliable information on threats, essential programs necessarily conducted in the field, and resentment against NGOs presence (indigenous versus refugees).


As 'NGO weaknesses,' the vulnerabilities are compared against strengths. It is important that this step be undertaken in detail so that all NGO vulnerabilities are noted. The comparison between weaknesses and strengths result in a list of factors that constitute the product of the Vulnerability Assessment.

RISK ANALYSIS

Risk Analysis is the core stage of the SRM. It is a method of combining all relevant information from the assessments by location and time to identify the possible impact and likelihood of each specific threat, which as a result, define the current <u>risk level</u>. It is not possible to conduct a Risk Analysis until the threats, programs and vulnerabilities of the NGO's activities have been assessed.

A rating system is necessary when articulating impact; likelihood and levels of risk for each specific threat. One- or two-word descriptors have been standardized within the InterAction SAG and are recommended. Rating systems are described in more detail at each step of the Risk Analysis.

Having completed the three <u>Assessments</u> you have now a clear image of the operational context in your Area of Responsibility. With this information, the Risk Analysis is conducted and includes each specific threat scenario; and all the factors from the assessments relevant to that threat go through two distinct steps.
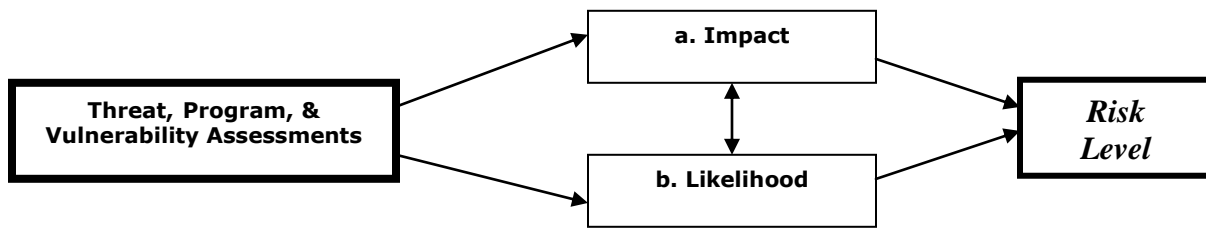
Graph 6 – Steps within the Risk Analysis

Impact

Each specific threat scenario is analyzed, within the context of the assessments, and the expected level of impact towards Operations; Personnel and Assets are identified and a descriptor is assigned to the threat. The expected impact may be determined from historical records of previous incidents, or similar situations from other countries. Descriptors for impact are in Graph 7 below.

Descriptor	Expected impact to NGO Activities:		
	Operations	Personnel	Assets
Negligible	Minor disruptions	No injuries	No damage
Minor	Limited delays	Some minor injuries / possible stress	Possible damage or loss
Moderate	Delays	Non life threatening injuries/High stress	Some loss
Severe	Severe disruptions	Severe injuries	Significant loss
Critical	Cancellation of activities	Death and severe injuries	Major or total loss

Graph 7 – 'Impact' Descriptors

Likelihood

Identifying the likelihood of each threat scenario is not an easy task.

It is at this stage of the risk analysis that the quality and precision of the previous assessment become critical. The use of statistics, experience, and recent history is the optimal method to determine the likelihood of a *threat scenario*. However, when those are unavailable, an estimate must be made.

For this purpose, the definition of likelihood includes the probability of the event happening under current conditions, and complementary guidelines on the required security and safety measures to be adopted by the NGO for each level.

When assessing a man-made threat, important efforts should be made to find and verify information that allows evaluation of the HIC of the organization or individuals responsible for the threat.

Likelihood is thus analysed with respect to two elements: a descriptor for the concept of e*vent probability* and *a percentage scale to be used as a general guideline*. One- or two-word descriptors are used to rate the likelihood of an incident occurring. Definitions for the descriptors associated with likelihood are listed in Graph 8.

Descriptor	Event probability	Guideline using a % scale	within a specific timeframe
Very Unlikely	Unrealistic	Less than 10% (less than 1 in 10)	every 5 + years
Unlikely	Improbable/Doubtful	Between 10 and 30%	Between 2 - 3 years
Moderately Likely	Reasonable	Between 30 to 60%	Between once a year / once a month
Likely	High	Between 60 to 90%	Once a week
Very Likely	Expected to occur	Over 90% (more than 9 in 10)	Daily

Graph 8 – 'Likelihood' Descriptors

Note: Determining the 'Likelihood' of an adverse event will often rely on the experience level of the security team (including the SMT) and shall utilize as much statistical and historical information as available. If an adversary has shown intent (or mind-set) to attack the NGO, and has known capabilities, together with a history of such attacks, the likelihood is most probably 'Likely.' If the NGO presents ample vulnerabilities in the area of the threat, the likelihood may be increased to "Very likely." The value and importance of the efforts made to validate and record information in the Threat Assessment step are clearly seen at this stage.

Risk Level

The InterAction SAG encourages the use of simple word descriptors to identify the levels of risk. These are from the lowest to the highest: *Very Low; Low; Medium; High; and Very High*. As in the process of evaluation of 'likelihood,' the definition of a Risk level often relies on the experience of the professionals involved. For a better understanding of each descriptor a table providing indicators for the expected operational context and recommended actions for each risk level has been developed.

	Characteristics of the general situation	Degree of concern for security	Continuity of operations	Mitigating measures
Very High	Extremely dangerous and unpredictable	Extreme	SMT and HQ decision	Implement immediate and extreme measures
High	Dangerous and unpredictable	Considerable	SMT and HQ decision	Implement urgent and very specific and robust measures
Medium	Dangerous but predictable	Significant	SMT and HQ decision	Implement significant measures
Low	Normally calm and predictable	Enhanced	Normal	Enhance current measures as required
Very Low	Calm and predictable	Routine	Normal	Current measures apply
	Characteristics of the general situation	**Degree of concern for security**	**Continuity of operations**	**Mitigating measures**

INDICATORS

Graph 9 – 'Risk Levels' Indicators Table

These indicators provide guidance to management, SMTs, professional security officers, and others involved in security decision-making for a precise Risk Analysis.

Having described all the components of the Risk Analysis, the next stage is to assign a current risk level for each specific threat by employing the Risk Analysis Table (See graph on page below).

Example of Risk Analysis *(See Graph 10)*
Specific threat: Direct threat of terrorist attack (what) on the parking lot of offices at xx (where) by VBIED (how), in the next 3 months (when); with the information available from the assessments, the impact and likelihood are identified;
Impact: evaluated as 'Severe' (under current conditions it may cause severe disruption to activities, severe injuries and significant loss of assets) – Likelihood: Identified as 'Likely' (high probability – 60 to 90% - of the event happening under current condition).
Both results are incorporated in the Risk Analysis table and the resulting current Risk level is identified as: High (There is a considerable degree of concern for the safety and security of personnel – The general situation is characterized as dangerous and unpredictable – The SMT will have to decide on the status of operations– Very specific and robust safety and security mitigation measures must be implemented).

RISK ANALYSIS TABLE	IMPACT				
	NEGLIGIBLE	MINOR	MODERATE	SEVERE	CRITICAL
VERY LIKELY	Low	Medium	High	Very High	Very High
LIKELY	Low	Medium	High	High	Very High
MODERATELY LIKELY	Very Low	Low	Medium	High	High
UNLIKELY	Very Low	Low	Low	Medium	Medium
VERY UNLIKELY	Very Low	Very Low	Very Low	Low	Low

(LIKELIHOOD is the vertical axis label)

Graph 10 – 'Risk Analysis' Example

The tool that you have for this step is the Risk Analysis Matrix. Using as a starting point each identified threat, extract from the assessments (PA-TA-VA) the relevant pieces of information needed to fill each box, and conduct a logical risk analysis on each threat. Having completed the SRA for all identified threats, the product will consist of a list of specific threats, grouped by location and time, with a specific risk level assigned to each.

The SRA matrix;

To facilitate the analysis and decision process, the use of a matrix is recommended. This matrix is called the "SRA Matrix." Columns are included for each of the stages of the SRA: Program Assessment (PA), Threat Assessment (TA), Vulnerability Assessment (VA), and Risk Analysis for the Mitigation Measures.

The "Realities"						The "Problems"			The "Solutions"	
Threat Assessment (TA)		Program Assessment (PA)		Vulnerability Assessment (VA)		Risk Analysis			Recommendations	
Threat	Situation	Location	Activity	Weaknesses	Strengths	Impact	Likelihood	Risk Level (current)	Mitigation Measures	Residual Risk Level (future)

Graph 11 – The 'SRA' (Security Risk Analysis) Matrix

The SRA Matrix can be used to show the overall impact of the combined risks to the NGO in a given country, area, or operation; or it can be used to assess a specific risk. It is also an excellent tool to summarize the SRA process and present the information to managers.

The grouping of risk levels by location and time will also provide information to identify risk levels for larger areas. Also the mapping of clusters of risks as identified in the SRA will help to identify the area risk level. This will support the decision for the selection of an appropriate security phase. It must be remembered that a security phase is simply another mitigation measure for a specific geographic area.

This product provides the necessary information to conduct the next stage of the SRA; the study of mitigation measures.
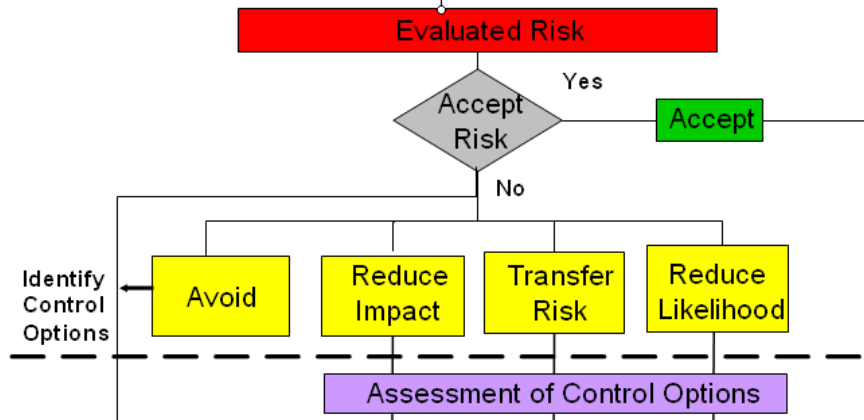
MITIGATION MEASURES

The concept of mitigation measures is simple: *To act upon identified factors of the operational context to produce a favourable change in the situation* enabling the effective and efficient conduct of activities while ensuring the security, safety, and well-being of staff as a high priority.

Using the SRM model, the Operational context has been clearly assessed in the Program, Threat, and Vulnerability Assessments. The NGO may act upon all factors, however acting upon the threat is difficult and sometimes beyond the NGO's capabilities. It is easier and more efficient to focus mitigation strategies on acting upon the factors that are under the NGO's control. Thus, in a good SRM exercise, most mitigation measures will be aimed at changing the NGO operational context by modifying elements of the Program or Vulnerability Assessment (see blue dotted lines on diagram below). This action will change the assessed risk levels (current) to the residual risk levels (future).

Strategies

Normally no single strategy will be able to cover all risks. A balanced list of strategies will usually provide the best solutions. Once the risks are identified, determine whether the risk is acceptable. If acceptable, no further actions are required other than to communicate and monitor the risk. If the risk is not acceptable it must be controlled through four separate options: reduce the impact, reduce the likelihood, risk transferral, and avoidance.

Accept   -   1. No further action

Control   -   Using prevention and/or mitigation measures
2. Reduce Impact
3. Reduce Likelihood
4. Transfer - Insurance, sub-contract, etc.
5. Avoid - Temporarily distance the target from the threat

The risk management strategy chosen will normally depend on the current risk level. In the table below are some suggested risk management strategies you may consider:

RISK ANALYSIS TABLE	IMPACT				
	NEGLIGIBLE	MINOR	MODERATE	SEVERE	CRITICAL
VERY LIKELY	Low (Control)	Medium (Control & Transfer)	High (Control & Avoid)	Very High (Control & Avoid)	Very High (Avoid)
LIKELY	Low (Control)	Medium (Control & Transfer)	High (Control And Avoid)	High (Control & Avoid)	Very High (Control & Avoid)
MODERATELY LIKELY	Very Low (Control)	Low (Control & Transfer)	Medium (Control & Transfer)	High (Control & Avoid)	High (Control & Avoid)
UNLIKELY	Very Low (Control & Accept)	Low (Control & Transfer)	Low (Control & Transfer)	Medium (Control & Transfer)	Medium (Control & Transfer)
VERY UNLIKELY	Very Low (Accept)	Very Low (Control & Accept)	Very Low (Transfer)	Low (Transfer)	Low (Control & Transfer)

Graph 12 – Example of application of mitigation strategies

Options

At this point of the process, decision-makers and security officials must determine what courses of action (or options) are possible to enable the programs while ensuring the safety and security of the organization, its staff, and its property. When evaluating, options must be reviewed in light of the risks and the program priorities established in the Program Assessment. For the SRM mitigation, options may include, among other measures: Security Phases; Policies, Training, and Partnerships. Efforts should be made to avoid producing a "shopping list" when presenting options for mitigation. Options must be feasible, funded, and include resources and timelines as far-out and detailed as possible.

For example:
- In order to Reduce Impact, some organizations in high threat areas utilize blast film over windows.
- Reducing the Likelihood can be accomplished though preconditioning supplies, so food distribution, for example, does not take place on a daily basis.
- To Transfer in an area where carjacking is common, an NGO may use a rental and hire a car service to lower its profile, thus transferring the risk of carjacking to the car service.

Always bear in mind that COST is not only money but also:

Culture –   *What will work in one culture may not work in another.*
Operational cost-benefit – A solution that is more expensive than the program, or which results in a high price tag for a small reduction of risk may not be the best option. Are there alternatives?
Systems –   *Any item of equipment will require people, training, facilities, support, maintenance, and multiple other factors to be available if it is to remain operational for the duration of its life cycle.*
Timeline –   *When is the mitigation option going to be available? What are we going to do until then? What will be the lifecycle?*

Mitigation strategies and options must be implemented with the aim to lower risk levels (reducing both impact and likelihood) of identified threats.

Expected "Residual" Risk Level

The risk level that is expected to remain present after the implementation of mitigation options is called the "Residual" risk level. It is based on this residual risk level that the Management and SMT will be required to make a decision on acceptability, and whether and/or how NGO operations and activities will be conducted in the locations where the identified residual risk exists.

Tip: After completing the Risk Analysis and having identified risk mitigation measures, you must now prepare the SMT and yourself for the approval of your recommendations.

Prepare the SRA summary
- List of threats and their associated current risks levels by priority;
- List of recommended mitigation measures, detailing how each measure (or set of) will address each threat and contribute to lower its current risk levels. List these by proposed date of implementation:
  - Immediate;
  - Less than 30 days;
  - Less than 90 days;
  - Less than 180 days.

 If easier for decision making, you may also list these organized by:
  - Common to all NGOs;
  - Program and organization Specific;
  - Location, installation or facility specific;
  - Activity/operation specific.

EXECUTION PHASE

The Execution part of the SRM model includes the next three stages: decision, implementation, and revision and update.

DECISION

This stage comprises three steps. It requires decisions to be made about priorities, logistical support, funding, and timeframes. Program pressures, financial limitations, contractor and host government delays, political ramifications and differing opinions make this stage extremely demanding. Correct decisions cannot be made without a concerted commitment to reduce risk, and a complete understanding of the consequences of not reducing risk.
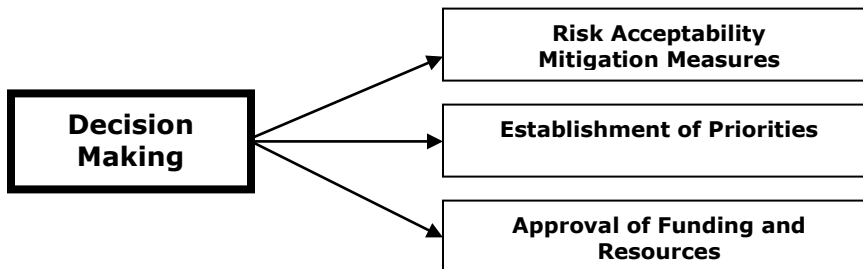
Graph 13 – Steps within the Decision Making stage

Risk Acceptability and Mitigation Measures

The SMT should discuss the identified risk analysis as prepared by the Security Focal Point (and Security cell wherever present). After which the SMT will evaluate the possible strategies and options to lower the current risk levels and reach residual risk levels with the purpose of enabling the implementation of program activities, then decide risk acceptability depending on the relative importance and criticality of each program.

IMPORTANT NOTE:
The determination of "acceptable risk" is a critical responsibility of senior managers within a Management System. The relationship between program criticality and the risk to personnel must be considered in the determination of "acceptable risk." Managers must constantly strive to balance these two critical functions and are accountable for creating a culture of security.

The Risk Analysis Matrix and list of recommended mitigation measures must be formally presented and discussed by the SMT.

Decisions on mitigation measures must be obtained and recorded in SMT minutes.
A Mitigation Measures Implementation Plan is prepared.

Establishment of priorities and timeframes

Not all elements of the selected option will be achieved at the same time, and priorities (i.e., for funding and construction) must be established. Moreover, time for implementation and completion of the selected options will be critical to reduce the risk to the organization and its personnel. Temporary risk mitigation measures may be required while projects are being completed. Examples include: reduced frequency of road missions, delays in implementing projects, or even temporary relocation of staff.

To support the next stage of the SRM model, a Mitigation Implementation Plan is developed. This plan is presented as a simple checklist designed to allow the tracking of the implementation process.

Specific Threat Scenario	Current Risk Level	Recommended Measures	Reduces		Approved by (date)	Priority	Observations / Comments	Ready (date)
			I	L				
	-		☐	☐		-		
			☐	☐		-		
			☐	☐		-		
			☐	☐		-		
			☐	☐		-		
			☐	☐		-		
			☐	☐		-		
			☐	☐		-		

Graph 14 – Mitigation Measures Implementation Plan form

The Mitigation Measures Implementation Plan must be approved and signed by all SMT members.

IMPLEMENTATION

The Implementation stage may involve alterations to NGO activities by cancelling or modifying some projects, whilst initiating others. It may involve the purchase of equipment, training of staff, or changes in personnel or to security phases. Decision-makers must be determined to implement the selected options as rapidly as called for.

It is not sensible to conduct the first six stages of the security risk management model only to delay or reduce support for its implementation. Without this stage operating effectively, the entire security risk management process will fail. Therefore, once the decision is made, there must be a strong commitment for implementing the mitigation plan. All progress and setbacks must be noted and actions taken as required.

IMPORTANT NOTE
A good SRA does not reduce the risk levels; it identifies these and assists in identifying possible solutions. Risk levels are reduced only *after* the mitigation measures have been implemented

A permanent follow up of the implementation of the mitigation measures is a duty of all management, SMT, and security focal points. The use of the Mitigation Measures Implementation Plan (Graph 14) provides an easy tool for this purpose. Periodically the management and the SMT must advise and be advised on the status of implementation. Periodical briefings on the status of the implementation process must be included.

REVISION AND UPDATE

After each safety and security related event, or when there is a significant change in the security environment, Best Practices require that such incidents be recorded and acted upon. This may result in updating or changing the SRA and incorporating previously unnoticed elements into the Assessments.

Update the SRA as needed in response to relevant changes in the operational context (including the implementation of approved mitigation measures), or as required. At a minimum, and in the absence of relevant changes in the situation, the SRA must be reviewed according to the requirements established by headquarters.

The trail provided by the sequence of documents of the SRM process, should show logical linkage between the SRA and the measures included in the Country Security Plan.

RECORDS AND REPORTS

To maximize the effectiveness of the method and to reduce the administrative requirements, the SRA must be prepared, presented, and reported in the most simplified format. The following is recommended:

Records:
- The Security Focal Point will prepare the Program, Threat, and Vulnerability Assessments and maintain at his/her office records of the information collected. There is no mandatory format for the Assessment files.
- Information collected in the Threat Assessment and expected to have important effects in the Risk Analysis must be validated and shared with the SMT and country management structure.
- SRA Matrix and Mitigation Measures Plan form should be shared with the SMT members, and the original filed.

CONCLUSION

Overall responsibility for the safety and security of NGO staff rests with the host government. However, accountability rests with managers at all levels, not only with their security focal points. Security focal points must provide the technical security inputs and advice that allows management officials to make informed decisions for managing security risks. Security risk management therefore requires good teamwork between those who plan and direct NGO operations and those who advise on the security measures which enable them.

The SRM model must be used as the primary security management tool to support the safety and security decision-making process. Its effective use allows the identification and prioritization of safety and security issues within the country office. Good security risk management practices call for updates as often as there are relevant "changes in the situation."

> *At the close of each Security meeting we should ask ourselves: "Will anything that we said or decided today result in a change in the risk level of a threat?" If the answer is yes, the SRA should be immediately updated to reflect those changes.*