**Step-by-step instructions to help you conduct a**

**Safety and Security Risk Assessment.**

|  |
| --- |
| **The steps of the SRA process are:**   1. Context Assessment (i.e., understand the big picture). 2. Identify and list the specific threats in the operational area. 3. Describe each threat. Then discuss vulnerabilities and existing mitigation measures. 4. Assess the likelihood and impact of each threat to the organisation (based on the above). 5. Plot the threats according to their risk level (likelihood x impact) in the risk matrix. 6. Identify mitigation measures for each risk. 7. Complete the security and safety risk table |

A Safety and Security Risk Assessment is aformal processused to identify and assess the security and safety risks of the working environment as well as the mitigation measures needed to protect our personnel, assets and operations from those risks**.** Its benefits can be phrased as follows:

1. **It helps to identify additional risks.** Doing a formal SRA usually facilitates the systematic identification of risks (including newly identified ones) and better mitigation measures. This is crucial to avoid important gaps in the security management system.
2. **It produces a more realistic risk assessment.** A formal assessment usually generates more realistic values (predictions) in terms of likelihood, impact and risk levels than informal risk assessments do. This, in turn, allows for prioritization of investments in safety and security.
3. **It helps raise awareness and buy-in among managers, staff, and volunteers.** The assessment is a group process that helps gain a more in-depth understanding of the threats that can affect staff and volunteers, and how all can work together to enhance safety and security. In our experience, staff and volunteers involved in an assessment process tend to be much more supportive of security training and measures.

**STEP 1: Context Assessment**

This step involves doing some research tounderstand the general context and threats before getting into the specifics.

This step is especially important when you are assessing a new area. If you are already very familiar with the area, you can go directly to step 2.

We recommend noting down the threats as you go. You can use the PESTLE approach to analyze the environment from different angles. PESLE stands for Political, Economic, Social, Technological, Legal and Environmental.

We also recommend that you do your research covering:

1. **External Factors:** Start by learning as much as you can about the country and area. Read up on its people, politics, geography, criminality, disasters, infrastructure, health facilities, etc. This information is usually easy to find in travel books and online.
2. **Internal Factors.** Find out as much as you can about your organization’s activities, operations, and teams. You need a good understanding of who is doing what, where and why before moving on to step 2. This information is normally available on request from your colleagues and organization.
3. **Actors and Relationships:** The activities and actions of other actors often impact our safety and security, so it is important to find out who they are, what they are doing and why. Other actors may include national government agencies, security forces, armed groups, UN agencies, NGOs and other Red Cross Red Crescent Societies working in the area. Some of this information can usually be found in previous versions of the security plan and on-arrival briefings but can also be researched online.

To have a good understanding of the context and make a preliminary list of threats that could impact the organization and its operations, please refer to document 01.1.1. (Context assessment table).

**STEP 2: Identify and List the Specific Threats**

The second step is to work as a group to identify all the threats in your operational area.

**Tips:**

1. **Do this as a group.** Groups with a diverse range of views, experience and backgrounds can identify more threats and vulnerabilities. Of course, if you are doing this in an emergency/disaster setting, you might have to do this mostly on your own through interviews. This is more time consuming and less effective, but sometimes it is the only option.
2. **Consider using a big map.** In our experience, one of the easiest and fastest way to identify threats in an area is to use a big map and to highlight all the locations and routes you might use. You subsequently enumerate threats pertaining to each location.
3. **Identify threats as specifically as possible.** For example, “crime” is too general, while carjackings and pickpockets are specific. Risks that apply to the whole area, such as recurring earthquakes, or political unrest should be listed at the top of the map.
4. **Do not get sidetracked by discussion.** Each threat will be discussed at a later stage, so simply indicate it on the map and move on.
5. **Do not discard threats raised by other team members.** At this stage, you should include every threat raised by the team, even if you do not think they are important. Every threat is assessed later in the process.
6. **Remember to include road, weather, disease, and terrain-related threats.** In insecure areas, we tend to focus on security threats and forget important safety and health threats.
7. **Remember: certain threats are not confined to specific geographic locations,** e.g., absence/failure of government institutions/services, economic recession, or a pandemic. These broad-reaching threats should also be included.

**Once you are done, you can compare your list to the non-exhaustive threat list in document 01.1.3.** You can also detail each risk.

Your list of the threats are entered them into the first column of the **safety and security risk table (document 01.1.2.).**

**STEP 3: Describe the Threats and Vulnerabilities**

Work as a group to describe each threat of your threat list (using the 5Ws described below) and attribute the vulnerabilities corresponding to each threat.

Do not spend more than 10-15 min to discuss each threat.

**The 5Ws and Vulnerability:**

* **Where** is the threat? For example, is it along a certain road, in a specific area or does it affect the whole area?
* **What/Who** is the source of the threat? For example, is it caused by a specific group(s), by some geographic features (ex: landslides), or by physical objects (ex: electrical wiring).
* **When** does it occur? Are threats more frequent or severe at a certain time of the day (ex: abduction at night), year (ex: flooding in winter), or concerning a specific event (ex: elections)?
* **Why** does it occur? For example, why do abductions occur? Is it because perpetrators sell kidnapped individuals on illegal markets? Is it for ransom? Is it politically motivated? Usually, there is more than one answer to the why question.
* **Vulnerability:** How vulnerable are we to this threat and why? For example, are we more vulnerable to this risk in a certain location or at certain times? Are some staff and volunteers more vulnerable due to their identity? Is our vulnerability linked to the lack of proper equipment, training, or information? Our vulnerability is often tied to mitigation measures we may or may not have in place.

In many cases, the risk assessment group will not have answers to all questions. Identifying gaps in our “security awareness” is still valuable information. Just make sure to note down information gaps and update the security and safety risk table once you have the answers.

**STEP 4: Assess Impact and Likelihood**

Use the scale below to determine the likelihood and impact of each risk on your list.

**Impact Scale :**

* **Critical:** Death, severe injury, loss of vital equipment, cancellation of activities
* **Severe:** Severe injury, possible death, loss of important equipment, major disruption to activities
* **Moderate:** Injury, loss of equipment, delay in activities
* **Minor:** Possible injury, possible equipment loss, limited delay in activities
* **Negligible:** Minor disruption to activities

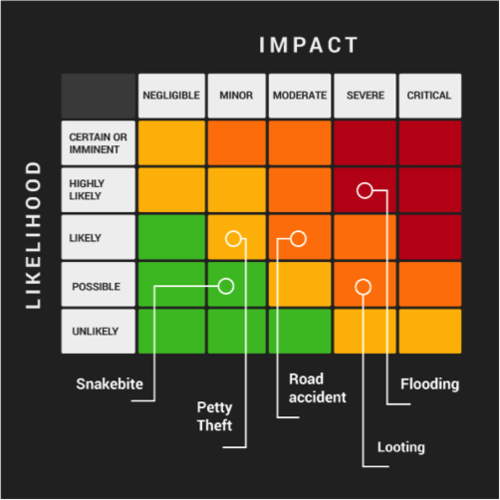
**Likelihood Scale :**

* **Certain or imminent:** Will occur or is actively occurring
* **Highly likely:** Has a very high probability of occurring
* **Likely:** Has a high probability of occurring
* **Possible:** Has a reasonable probability of occurring
* **Unlikely:** Is unlikely to occur to Red Cross Red Crescent staff members or volunteers

Once you determine the values regarding the scales (Impact; Likelihood), you enter them into the you enter them into the third and fourth column of the **safety and security risk table (document 01.1.2).**

**STEP 5: Plot the risks in the risk level table**

Use the impact and likelihood values from step 4 to **plot the risks** in the risk level table, as shown below. Using a table helps us visualize and prioritize the risks within a given operational area. It also helps us identify risks that exceed your organization security threshold (those in orange and red) and that will require additional mitigation (see step 6).



All the threats should be plotted in the risk level table, as shown above, and ranked as follows:

* Threats in the red area = Extreme Risk
* Threats in the orange area = High Risk
* Threats in the yellow area = Moderate Risk
* Threats in the green area = Low Risk

You should have a combination of values for likelihood and impact according to each threat. You can enter them and color code the risk levels into the fifth column of the **safety and security risk table (document 01.1.2.).**

**STEP 6: Identify Mitigation Measures**

For each risk, identify the **existing** and **additional** measures required to mitigate the risk to an acceptable level (green or yellow). You can also divide them per passive mitigation measures (reducing the risk of an event from happening) and active mitigation measures.

The mitigation measures should **reduce both the likelihood and impact** of a threat.

Threats that fall into the **orange and red** areas of the table (high-extreme risk) **are usually deemed above the risk threshold** and require urgent treatment (mitigation measures to reduce the risk to yellow).

It is important that you inform the Senior Field Manager (e.g., country director) and your security advisor if you identify high or extreme level risks.

You can list the mitigation measures into the sixth and seventh column of the **safety and security risk table (document 01.1.2).**

**STEP 7: Fill-out the Security and Safety Risk Table (document 01.1.2)**

|  |
| --- |
| Proposed structure of the table :   * Column 1: Threat Name (from step 2) * Column 2: Threat Description (from step 3) * Column 3: Likelihood Description (from step 3) * Column 4: Impact Description (from step 3) * Column 5: Risk Level (from the table in step 5) * Column 6: Existing Mitigation Measure (from step 6) * Column 7: Additional Mitigation Required (from step 6)   Fill out the other parts of the SRR such as the date and names of persons who conducted the assessment. Then, submit it to your management and security for review and follow-up. |

**What happens next?**

The final step is taken by management and is often referred to as the “risk evaluation” step (according to ISO standards). In brief, the management team will use the information derived from the security and safety risk assessment to evaluate the risks and decide which risks need to be “treated” (reduced to an acceptable level). Decisions may include:

•  Whether a risk needs treatment.

•  Priorities for treatment.

•  Whether an operational activity should be put on hold.

Risk treatment measures may include the writing (or updating) of procedures, guidelines, and plans; investing in training; acquiring of equipment; restricting/avoiding activities or travel in some areas:

Risk treatment measures are captured in the safety and security risk table and usually assigned to a manager for implementation within a given deadline.