



United Nations Security Management System

Security Risk Management (SRM) Manual

Issued 11 December 2015

TABLE OF CONTENTS

Introduction	1
Conceptual Overview	3
PART I: Introduction to Security as Risk Management.....	3
PART II: The Structured Approach to SRM.....	9
Step 1: Geographical Scope and Timeframe	11
Geographical Scope.....	11
Timeframe	11
Step 2: Situational Analysis	13
Step 3: Programme Assessment	17
Step 4: Threat Assessment	21
PART I: General Threat Assessment.....	21
PART II: Specific threats and event descriptions.....	26
Step 5: Security Risk Assessment	35
The Concept of Likelihood in the UNSMS	35
Prevention Vulnerability Assessment.....	36
Impact	38
Mitigation Vulnerability Assessment	39
Risk Levels	40
Step 6: Security Risk Management Measures	44
Projecting Required SRM Measures	44
Selecting SRM measures	44
The effects of SRM Measures - reducing Likelihood and Impact	46
Integrated Systems Approach.....	47
Decision-making and Implementation.....	48
Step 7: Security Risk Management Implementation	52
Step 8: Acceptable Risk	56
Acceptable Risk Model	56
Programme Criticality Tool.....	58
Step 9: Review and Monitoring	59
Security Risk Management Areas Monitoring and Review	60
Support: DSS Guidance on SRM Process Management, Support and Oversight	65
SRM Flow Process	65
SRM Support and Oversight.....	65
SRM Confidentiality.....	677

Annex A: Glossary	688
Annex B: Programme Planning Cycle	700
Annex C: Programme Criticality Tool	722
Annex D: General Threat Assessment Definitions and Security Levels.....	888
Part I: Definitions of Descriptors in the General Threat Assessment.....	888
Part II: The General Threat Assessment and Security Levels	944

Introduction

Introduction

Security Risk Management (SRM) is a United Nations Security Management System (UNSMS) analytical process for assessing the operational context of the UN in order to identify the risk level of threats that may affect UN personnel, assets, premises and operations on the basis of which, security management decisions are made. The SRM process was first launched by the UNSMS in 2004. Since then, it has been updated in a new UNSMS policy in 2009 and there have been multiple additional related guidelines, training tools and templates intended to improve the process.

In July 2010, the Inter-Agency Security Management Network (IASMN) formed a working group with the original purpose of examining ways to improve likelihood assessments within the Security Risk Management (SRM) model. The working group included senior security professionals from DSS and several UN organizations, from the field and headquarters.

In January 2011, the IASMN, cognizant of the need for broader enhancements of the SRM process, expanded the remit of the working group beyond the area of likelihood assessments to include the entire SRM process. Reviews of Security Risk Assessments (SRA) and the resulting recommendations and decisions indicated that the following areas could be further enhanced:

- The reliability and validity of security risk assessment;
- The context-specific security risk management strategies;
- Structured decisions for acceptance of risks;
- Dynamic, responsive and flexible application of the SRM process, to changes in the situation and programming.

These improvements, among others, will result in increased trust in the SRM process and as a tool to better enable security advisors and decision-makers to effectively manage risk.

This Manual combines policy, guidelines and technical instruction on SRM that any user should be able to use to expand their knowledge of the theory and practice of SRM in the UNSMS.

The Manual contains new concepts and definitions and will guide users in applying the SRM process. Even though the SRM is a component of all UNSMS policies, guidelines and procedures, this Manual does not address all aspects of security management in the UNSMS. Reference is, therefore, made to the Security Policy Manual and the Security Management Operations Manual.¹

The Manual is structured to follow the sequence of the SRM process. After the introduction and conceptual overview, each chapter of the Manual deals with a distinct step in the SRM process discussing the theory behind it, a

¹ See <https://unsmin.dss.un.org/unsmin/Library/PolicyandProcedures.aspx>

clear explanation of the components of each step and ends with a snapshot of the UNSMS SRM tool. Once readers have familiarized themselves with the details of this Manual, they will have the knowledge and tools to apply the SRM process to their work environment covering a broad spectrum of the work of the UN.

Outputs of the SRM process are:

1. A Security Risk Management Area or Ad-hoc SRM document;
2. An overview Designated Area Security Risk Management document (previously referred to as the “Country SRA”);
3. A change summary document and;
4. An SRM document in support of decisions regarding specific programme, premises or activities associated with unique threats.

Conceptual Overview

Conceptual Overview

PART I: Introduction to Security as Risk Management

The purpose of this chapter is to introduce readers to the main concepts involved in risk management and how risk management is applied to security in the United Nations Security Management System (UNSMS).²

The terms risk and risk management have been commonly used to apply to other components of the United Nations system, including business continuity, emergency preparedness, and audit. Despite their increased use, or perhaps because of it, the terms and the processes they encompass are not clearly or commonly understood. That is why it is necessary to explain what Security Risk Management means, why it is important to the UNSMS, and how it uses a simple but structured decision-making model to help the United Nations system better achieve its goals.

What is Security Risk Management?

Security Risk Management is our system of identifying future harmful events that may affect the achievement of objectives: assessing them for likelihood and impact; and determining an appropriate response.

Any United Nations objective, from global strategic goals to local programme plans, may fail because of various obstacles. In the security context, obstacles are called threats. All managers must identify threats and evaluate how these threats may affect their objectives. In many of the places where we work, the effect of threats, if not managed, can be fatal to personnel and programmes.

Risk, on the other hand, is the combination of the likelihood of a threat being carried out and the subsequent impact for an organization. The process whereby a manager identifies, evaluates and systematically deals with obstacles to success is risk management. Security measures can either be used to prevent a vulnerability from being exploited or mitigate the impact of an exploitation, or both. One way to think of risk management is that it is the systematic determination and implementation of timely and effective approaches for managing the effects of threats to the organization. Security Risk Management is merely the management of security-related risks³.

Why is it Important?

Security Risk Management is an essential management tool. It increases our chances of achieving our goals by decreasing the effect of threats. Security Risk Management offers a structured approach to help make good decisions and allows for clear accountability. It allows managers to maximize

Key Definition

Risk management: The systematic determination and implementation of timely and effective approaches for managing the effects of threats to the organization.

² Who is covered by the UNSMS is found in *Security Policy Manual*, Chapter III, “Applicability of the United Nations Security Management System”.

³ Many United Nations organizations have a dedicated risk management approach that deals with risks beyond those categorized as “security risks”. Often that system is called Enterprise Risk Management.

programme opportunities and to allocate security-related resources in ways that enable programme delivery within acceptable levels of risk. It is vital to achieving the planned and envisioned programme results for the organizations, especially in complex and dangerous environments.

Definition of “Risk”

Key Definition
Risk: Risk is the likelihood of a harmful event occurring and the impact of the event if it were to occur.
(Risk = Likelihood x Impact)

Although the steps of Security Risk Management are clear and simple, it is important to understand what “risk” is. The UNSMS has adopted the concepts of Likelihood and Impact to define Risk; the assessment of Risk, therefore, is an assessment of how vulnerable the Organization is to an undesirable event (a Threat), expressed in terms of Likelihood (the prospect of the event occurring) and Impact (the effect of the event if it does occur).

Key Definition
Likelihood: A rating of the assessed potential for a harmful event to effect the Organization.
Impact: A rating of the assessed potential harm that an event would have (if it were to occur) on the Organization.

To illustrate, risk is intuitively composed of two components (Likelihood and Impact), take the example of a tightrope walker - most people have little hesitation walking along the top of a table or bench. If you raise the table or bench 100 feet/30 meters in the air, most people would feel very uncomfortable doing the same thing. This is because they intuitively know that the risk has changed. Even though the likelihood of falling off the table is the same in both situations, the impact (if they were to fall) in the second situation is significantly higher. If the table is shrunk to the size of a rope, as it is for a tightrope walker, then the likelihood of falling also increases. Thus, the risk from falling is a combination of both the likelihood of falling and the impact of the fall.⁴



Understanding that risk is a combination of likelihood and impact, it is clear **that managing risk is a question of managing likelihood and impact.**

A tightrope walker may use a large pole to increase his balance and lower the likelihood of falling. He may also install a net below the tightrope so that if he does fall, the impact will be less serious. In this way, he has managed his risk by managing both likelihood and impact.

Key Definitions
Taking measures to reduce **likelihood** = “**Prevention**”.
Taking measures to reduce **Impact** = “**Mitigation**”.

When discussing the management of risks, the UNSMS has adopted the terms “Prevention” and “Mitigation”; taking measures to reduce Likelihood is called “Prevention”⁵ while taking measures to reduce Impact is called “Mitigation”.

In the Security Risk Management process in the UNSMS, Likelihood and Impact have unique definitions, distinct ways for being measured and a common way of being combined to determine risk. This is explained in greater detail in Chapter 5 of this Manual. At this point, it is important to understand that Likelihood and Impact are assessed on a 1-5 scale and combined in a Risk Matrix as follows:

⁴ In this example, you are “the organization.” The risk to another organization from you falling will be different because the impact may not be the same.
⁵ Technically, measures meant to reduce likelihood rarely bring likelihood to zero. Therefore, they don’t really “prevent” the event, in that they do not make it impossible for the event to occur.

Risk Matrix	Impact				
	L I K E L I H O O D	Low	Medium	High	Very High
Low		Medium	High	High	Very High
Low		Low	Medium	High	High
Low		Low	Low	Medium	Medium
Low		Low	Low	Low	Low

Figure 1: Risk Matrix

Threat, Risk and Vulnerability

Key Definitions

Threat: A potential cause of harm initiated by deliberate actions.

Hazard: A potential cause of harm resulting from non-deliberate actions.

Vulnerability: A weakness that can allow a threat or hazard to cause harm.

To conceptualize Threat, Risk and Vulnerability, it is helpful to use another example, this time involving our ancestors. *Generations ago, our human ancestors lived with the very real danger of attack by predators. They saw members of their communities killed by predators, and knew the **threat** was there. Changes in nomadic life and in the environment meant that humans interacted with predators to various degrees and often competed with them for scarce resources. Coexisting in the same environment with predators increased the **likelihood** that humans would be attacked by these predators, including the possible worst **impact** of being killed. As well, human physical prowess was a significant weakness or **vulnerability** compared to some predators.*

*What did our ancestors do to **manage** the risk posed by predators? They avoided areas where predators were common, and they developed protection strategies against predators when they needed to gather food or water. Protection strategies included living in groups, sleeping in trees when travelling, building shelters to keep predators out, and even developing weapons to repel or kill predators when required. Some **prevention measures lowered the likelihood** they would be attacked, such as building shelters, while **mitigation measures lowered the impact** if they were attacked, such as communicating between groups to call for help and developing responses to help the injured. Through all this, they found a balance between what they needed to do and the threat posed by predators.*

We control our risk by controlling our vulnerability to risks. In this way, the goal of risk management is to lower our Vulnerability thereby lowering Likelihood and/or Impact. When we lower Likelihood through prevention, this is also called changing the “Prevention Vulnerability”. When we lower Impact through mitigation, this is called changing “Mitigation Vulnerability”. There are hundreds of similar day-to-day examples of how we manage risk in our daily lives.

This is one of the most important issues for SRM: management decisions must not be based on the threat! Only when we are clear on our vulnerability to a threat should we decide what to do next.

Clearly, our ancestors’ decision about whether they should go into an area where predators hunt was not based only on the fact that the predators were in the environment. The decision should also reflect our realistic evaluation of our present vulnerability to the threats in that environment (what effective

protection measures they had) and our ability to decrease our vulnerability through increasing our protection. This is one of the most important issues for SRM: management decisions should not be based on the threat! Only when we are clear on our vulnerability to a threat should we decide what to do next.

The decision to go ahead with an activity would also consider how important the activity is. *Our ancestors may travel through predator-infested areas to gather food for their children or to come to the aid of others in their communities. They may not, however, take the same risk only to gather items for a cultural ceremony.* This is an issue of Acceptable Risk and the balance of risk and benefit (in the UN system, the “benefit” is called “Programme Criticality”). This will be addressed later in this Manual.

Risk Management Strategies

Risk management is the process whereby an organization attempts to lower Risk by influencing Likelihood and/or Impact. Because we have little or no influence over the threat, it is best to concentrate on lowering Risk. Influencing Likelihood and Impact is usually done through what is known as “risk controls”. There are, however, other ways to manage risk besides just “controlling” it. In fact, there are four main strategies for managing risk (ACAT):

There are four main strategies for managing risk (ACAT):

- Accept
- Control
- Avoid
- Transfer

- Accept the risk (no further action)
- Control the risk (using prevention and/or mitigation measures)
- Avoid the risk (temporarily distance the target from the threat)
- Transfer the risk (insurance, sub-contract, etc.)

These four strategies will be explained in more detail in Chapter 8.

Deliberate vs. Non-deliberate Events

In assessing and managing risks, it is important to realize that there is a difference between events purposely caused by a motivated human antagonist and events that are acts of nature or accidents. In the SRM process, the former are called “Deliberate Events” and the latter are called “Non-deliberate Events”.

The “cause” of deliberate events is a “threat”. The “cause” of non-deliberate events is a “hazard”. In the UNSMS, the concept of “security” covers threats (Deliberate Events) and the concept of “safety” covers hazards (Non-deliberate Events). See Table 1 below.

Subject	Type of “danger”	Types of events
Security	Threats	Deliberate
Safety	Hazards	Non-Deliberate

Table 1: Security vs Safety

What hazards are not part of the UNSMS SRM process?

Although most human-caused, deliberate events are covered under the concept of “security”, not all non-deliberate hazard events are covered under the “safety” remit of the UNSMS. The UNSMS only has the remit for three areas of safety: road safety, fire safety and aviation safety. Thus there are many other areas of safety not covered by the UNSMS (and, therefore, the SRM process), including medical issues such as disease, occupational health and safety, and structural engineering.⁶

The Steps of Security Risk Management

The Security Risk Management process is a structured, problem-solving mechanism. It is a nine-step process:

Step 1: Setting the geographical scope and timeframe

Where will we be working and what is the timeframe for the analysis?

Step 2: Situational Analysis

What is the overall security situation in that area?

Step 3: Programme Assessment

What are the main programme goals and posture in that area?

Step 4: Threat Assessment (General & Specific)

What are the obstacles to achieving goals?

Step 5: Security Risk Assessment

How vulnerable is the Organization to these threats?

How will they affect the Organization and which threats require the most attention?

Step 6: Security Risk Management Decisions

What can actually be done about these risks?

Step 7: Security Risk Management Implementation

Procedural and budget aspects of implementing the agreed security risk management measures

Step 8: Acceptable Risk

Is the risk acceptable in balance with the criticality of programme

When it comes to deliberate events, the UNSMS does not use “Quantified Risk Assessment” (QRA). QRA uses mathematical probability and other techniques to calculate risk. This approach requires large data sets, expertise in mathematics, and is extremely challenging for changing, “open” systems, such as human violence.

The SRM process, therefore, uses a structured subjective model to assess risk. In this way, the SRA is not about predicting the future but about organizing our thoughts about it, creating a relative/comparative risk prioritization rather than an absolute and accurate assessment of Likelihood and Impact. Many experts believe that a “pure”, accurate measurement of risk is impossible to achieve and attempts to do so creates a false sense of security.

⁶ As noted in footnote 1 above, other risk areas are usually covered by an organization’s Enterprise Risk Management and/or Occupational Health and Safety processes.

Important!

All structured tools open themselves up to manipulation. **At no time** should any of the options in any of the steps of the SRM Process be chosen in order to achieve a desired result from that step or any other end result. Any attempt to “retro fit” an assessment will corrupt the whole SRM process.

activities?

Step 9: Follow up and Review

Are the measures working? Is the assessment of risk now similar to how it was projected?

Security Risk Management in the UNSMS follows these basic steps with a unique tool to assist in each step.

Each step of the risk management process and how each step interacts with other steps is explained below.

Figure 2 shows the main steps in a circular pattern reflecting the cyclical nature of the process.

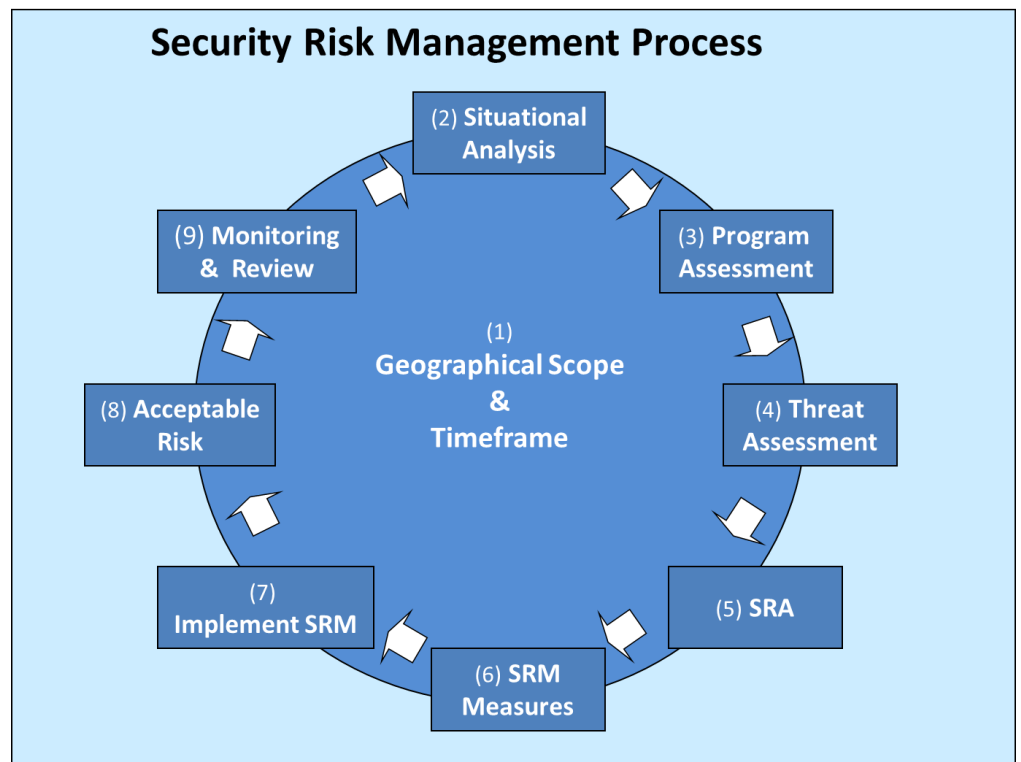


Figure 2: The Risk Management Cycle

FOR MANAGERS! Because risk-management decisions include concerns of cost and benefit, as a manager, you are well placed to discuss such issues. Although managers may worry about the costs of risk management, it is also important to consider the costs of not managing risks. Not managing risk can be unacceptably expensive because undesirable events have more than just a primary impact on the organization. Risk events will always have secondary and tertiary costs. Therefore, risk management may save money by lowering loss.

PART II: The Structured Approach to SRM

Human beings make subjective risk evaluations daily, but research shows that these evaluations are often inaccurate. This is because risk can be counter-intuitive. A common error is the “optimistic bias”, whereby people believe that they will not be the victim of an undesirable incident because it has never happened to them before. Most people find it impossible to imagine themselves as the victim of a dangerous event and say “it can’t happen to me.” Another common error is “danger habituation.” As the dangers increase, people get used to them, become complacent and neglect to take the necessary security precautions. Because people’s perceptions of risks vary so widely, various decision-makers in an organization may not be making risk decisions in line with an organization’s overall risk strategy. These errors can lead to unnecessary programme cancellation, or worse, unnecessary death or serious injury of personnel.

Here are a few examples of the dangers of subjective risk evaluations:

- As I have never had a mobile phone stolen from me before, it should be safe to carry mine hooked onto my belt, even though the area I am entering appears rather seedy.
- I don't need extra bars on my windows and doors as no intelligent person would attempt to break into my house as I am a big person with a powerful physique.
- It is not a problem checking into a cheap hotel in a questionable neighborhood as the locals will not want to attract the attention of the police by robbing me.
- I don't require additional measures when visiting the primary schools in the volatile region, as local culture would never permit an attack there because children may be killed or injured.

To reduce the problems that come with subjective risk evaluations, risk needs to be assessed in a structured way. A structured approach ensures a more comprehensive analysis, leads to better decisions, and limits errors in subjective evaluations and biases.

The analytical concepts behind the assessments done in the SRM process are called Decomposition/Deconstruction and Externalization.

- "Decomposition/Deconstruction" breaks the problem down into its component parts. In the SRM process, most steps are “decomposed” into as few variables as possible, with precise definitions of terms that allow for approaching the problem in a standard way. An example of this is how Risk is “decomposed” into Likelihood and Impact.
- "Externalization" takes the problem and puts in into a format that can be visualized and adjusted in a standard, structured way. As you see how the various steps in the SRM process are done, you will see there is always a tool to help “externalize” the variables and your assessment of them.

The aim of the structured approach in the SRM is that the process be:

- Fact-based, logical, and systematic
- Globally applicable in a consistent, de-politicized manner
- Reliable (achieve similar results when different people use it)
- Valid (accurately represent the security environment on the ground)
- User-friendly without being over-simplistic

By conducting the analysis in this manner, it is more likely that an analysis done by different people for the same location will be consistent. The structured nature of the process provides a basis for specific discussion of differences when they arise. Finally, structure allows the process of assessment to be more efficient, freeing up time for security practitioners to understand and analyze the security environment and the problems it contains.

Having an assessment “externalized” onto a matrix, for example, with each assessment represented by numbers, also allows for a “validity check”. This is a check to see if there are any anomalies or differences that stand out between issues being assessed. This process will be discussed in more depth later in the Manual.

All structured tools open themselves up to manipulation. **At no time** should any of the options in any of the steps of the SRM Process be chosen in order to achieve a desired result from that step or any other end result. Any attempt to “retro fit” an assessment will corrupt the SRM process.

Conclusion

For managers to achieve their organizational goals, they must approach security risk in a structured way. The risk-management approach to security laid out in this Manual simplifies security risk management; and saves costs by managing security risks effectively.

Having explained the general concepts of Risk and Security Risk Management, we can go into detailed guidance on how to accomplish each step of the Security Risk Management process.

Step 1: Geographical Scope and Timeframe



STEP 1: Geographical Scope and Timeframe

Geographical Scope

Risk management in the security context deals with threats in the environment. Therefore, it is important to determine a specific area in the environment in which these threats occur. It is also necessary to establish clear geographical locations to set the context in which programme and vulnerability assessments are made. The establishment of the geographical scope of the SRM process is the key first step.

If the geographical scope is too broad, then the threat and risk assessments will have little meaning. Too many small areas will require the use of the SRM process in too many areas and create unnecessary work.

The general guideline is that the selected geographical scope should contain similar characteristics. *For instance, if a country contained a large capital city in which UN offices were located, a region of widespread drought in the east of the country and an area in which IDPs were located, it would make sense to treat each of these three areas as a separate security risk assessment.* The political division of a country as established by the government may not be the best way to establish geographical scope for the SRM process.

Key Definitions

SRM Area: Geographic scope defined for the application of the SRM process

Timeframe: The time into the future that the present **analysis** in the SRM Process can be expected to be valid.

It is important to note that the UNSMS uses three layers of geographic scope:

- The first is the “**Designated Area**”. This is the area assigned to a Designated Official (DO) by the Secretary-General. This is usually equivalent to the country, but isn’t always. Examples exist where one country is divided into two or more Designated Areas under the responsibility of two or more Dos or where a DO covers more than one country.
- The second is the “**Security Area**”. All Designated Areas must have at least one Security Area. Where there is no ASC designated the Security Area is the same as the Designated Area. Where ASCs are designated their area of responsibility is the Security Area.
- The third is the “**SRM Area**”.⁷ This is the area of homogeneous threats for which an SRM assessment is carried out. The determination of an SRM area is the decision of the DO/ASC in consultation with the SMT/ASMT. All Security Areas must have at least one SRM area. An SRM Area must lie within a single Security Area⁸.

Timeframe

Establishing a clear timeframe for analysis is very important for the SRM process, especially in regard to discussions on likelihood. It is important to

⁷ Formally known as “Security Level Areas”.

⁸ First use of E-Tool – The default in the E-Tool is to use the currently established SLA as the SRM areas. If the SRM areas are to be changed then this should be addressed to the DSS Desk Officers.

clearly specify the time frame under consideration because different durations of time are likely to be related to different levels of opportunity to carry out threats. The question is how likely the event is to occur within an established timeframe

Over a longer time frame a threat may be harder to quantify. For example, an assessment about whether an individual is likely to carry out a threat against the UN, such as a bombing, at some point in the future is likely to be less useful when managing a risk and in prioritising resources, compared to assessing the likelihood of a bombing within a clearly specified time frame such as the following six months. By focussing on the next six months, it may be possible to more accurately evaluate the likelihood of the event. In the context of terrorism the time frame may be of additional importance given that terrorist groups on occasion may work towards specific dates, e.g. specific anniversaries. Similarly, external events such as elections or UN programmes and operations may drive the timeframe set for the assessment.

For the SRM process, a very wide set of analysis timeframes can be used - from one day for a road mission to 12 months. No timeframe for analysis will extend beyond one year (12 months) to ensure that threats are constantly re-evaluated. For SRM Areas where the security threats are prone to change rapidly, a timeframe of, for example 3 or 6 months, is recommended. For SRM Areas where the security threats are more stable, a longer timeframe (for example 6 or 12 months) is recommended.

When the SRM process is applied to a short mission, such as a programme activity, then the time frame should match the timeframe of the mission.

Once established at this stage of the SRM process, the geographical scope (SRM Area) and timeframe will apply to all other steps of the process. Multiple SRM processes can be combined into a designated-area SRM report.

UNDSS Security risk management e-Tool

Step 1: Geographic Scope and Timeframe

SRM area: Yemen (Yemen) Sana'a

Period from: 05-Nov-2015 to: 04-May-2016

Launch SRM process

	Time frame	Created by	Status	Status date
View Edit	05-Aug-2015 06-Aug-2015	Alejandra Barcelo IMF	In Progress	05-Aug-2015
View	01-Jul-2015 31-Jul-2015	Igor Jankovic DSS	Submitted to DO	15-Jul-2015
View	01-Feb-2016 29-Feb-2016	Igor Jankovic DSS	Approved by DO	09-Jul-2015
View	25-Jun-2015 30-Jun-2015	Simon Butt OCHA	Approved by DO	09-Jul-2015
View	25-Jun-2015 31-Dec-2015	Michael Jay Dell Amico UNHCR	Approved by DO	24-Jun-2015
View	25-Jun-2015 29-Jul-2015	Simon Butt OCHA	Approved by DO	24-Jun-2015
View	01-Jan-2016 31-Jan-2016	Milan Simeunović DSS	Approved by DO	24-Jun-2015
View Edit	23-Jun-2015 30-Jun-2015	Maarten Daman ICJ-CIJ	In Progress	24-Jun-2015
View	13-May-2015 16-Jun-2015	Simon Butt OCHA	Approved by DO	24-Jun-2015
View Edit	18-Apr-2015 18-Jul-2015	Simon Butt OCHA	In Progress	11-May-2015
View Edit	01-Mar-2015 01-Jun-2015	Igor Jankovic DSS	In Progress	11-May-2015

Figure 3: Computer Tool – Geographical Scope and Timeframe

Step 2: Situational Analysis

STEP 2: Situational Analysis

Overview



Familiarity and knowledge of the general security situation are of prime importance when applying the SRM process. The SRM assessment must be based on facts and the facts must be relative to the environment in which the UN is working. Using the steps and tools contained in this Manual without a detailed understanding of the security environment, or using incorrect or erroneous information, will lead to inappropriate, and perhaps dangerous, security decisions. To ensure that you have the required knowledge of the security situation in the SRM Area under analysis, the next step of the SRM process is the completion of the Situational Analysis.

Reminder

This outline does not imply a lengthy discourse on any of the listed topics. The SRM tool is designed to simplify the SRM Process. In this vein, include only the level of detail necessary on any topic to support the overall SRM Process.

The situational analysis is a collection of concise narratives that aim to illustrate and identify the drivers of insecurity in the environment. It is this narrative overview of the current security situation that “sets the scene” and provides the context for the structured subjective assessments to follow. Most importantly, it provides a common understanding of the environment from the security perspective for the security decision makers.

Some of the points in a situational analysis may cover the whole country, while others may only apply to a specific SRM Area. The extent of the Situational Analysis will depend upon the reason for which the SRM is being applied. For example, the Situational Analysis of a SRM process for a specific project, programme or operation may refer to the broader, more comprehensive Situational Analysis in the Country RMA, or a shorter, more focused situational analysis may be done for a quick one-off, time bound risk assessment.

Since the SRM process is addressing the current situation and managing current risk, historical details should only be included when they have a direct impact on the current environment. When composing the narrative the author needs to be constantly aware of the question “*so what impact does this have on security*”; if the answer is that it does not impact the security environment then it does not need to be included.

The level of detail in the situational analysis will depend on the information available, the analytical capacity of the security team and the complexity of the security environment. There are eight (8) key areas that need to be considered but if any of the areas has no impact on the security situation they do not need to be unnecessarily expansive:

1. **Political.** This section addresses the political make-up of the country in general, and the SRM Area in particular. (if applicable only to a smaller portion of the country). Political in this sense does not mean an analysis of the politics of the country, but rather an analysis of the various factors which make up the political landscape. These could include the stability of the government, the quality of the bureaucracy, information about groups with competing claims over rights or resources, any conflicts within or outside the country that could affect the operating environment. Conflicts could be internal (including civil war, terrorism, civil disorder and/or religious or ethnic tensions) or external (e.g., conflicts in neighboring countries and cross border conflict). There is

Warning: Any discussion on the quality of governance and accountability is extremely sensitive. Bear in mind that you may not have control over who may later read this document. Be cautious about phrasing in a way that could be construed as United Nations interference in the government of the country, and which could lead to possible actions such as PNG.

no fixed list of topics under this heading, and a thorough knowledge of the historical and current political dynamics is required in order to successfully isolate those factors which may affect security.

2. **Economic.** In many countries, economic factors are one of the main drivers of instability. The work of the UN is therefore very dependent upon understanding these economic factors and how they may affect the identification of threats. Economic factors may result in the presence of IDPs, crime, urban or other internal migration, or the relative economic primacy of a specific group over another. It is important however to note that this is not a detailed analysis of the economy, but rather a brief description of the economic situation as it affects the stability of the country and more specifically the safety and security of the United Nations. It may still be necessary to briefly describe whether the currency is under threat; the most recent trends in economic factors; which groups or sections of the populations hold the majority of the wealth; and, whether the country is in need of significant foreign/donor assistance to prop up a weak economy. It is not expected that this will be a lengthy section of the Situation Analysis.
3. **Social.** The social fabric of a society has a significant effect on the safety and security of UN activities. One of the main manifestations of the breakdown in societal norms is crime, and therefore law and order together with crime form the basis of the discussion under this heading. Other important elements of the analysis of society are the ethnic; cultural; religious; economic; age and gender distribution of the population; educational breakdown of the population; as well as the main social issues on the national agenda.
4. **Environmental.** This section is used to describe the physical attributes of the SRM area, keeping in mind the description is for the purposes of later identifying the relevant security threats. Scarcity of water, flooding, avalanches, extreme weather conditions, earthquakes, and typhoons for example should be described as they impact on security. Describe the land covering such as surface area, vegetation, forests, deserts, plains, rivers and lakes etc. with the aim of describing how geography and climate affect UN personnel, premises and programme delivery. Frequency and geographic distribution of natural disasters are important as these types of events frequently affect limited areas for limited periods of time, and are not continuous. The analysis of the environment has only one purpose; which is to understand environmental factors that may affect security.
5. **Infrastructure.** Infrastructure is very important to both UN programme delivery and the economic well-being of the country. This section describes the infrastructure, meaning the man-made components of the country, rather than its natural geography. The discussion should include the following items if they affect UN security: transportation, telecommunications, media, internet access, electricity and housing.
6. **Country Security Forces.** A description of the security forces is essential to understand the inhibiting context later in the SRM process. This section should be divided into military, police and corrections subsections. For peacekeeping missions, a discussion of Peacekeeping

Tip: Bear in mind that our locally recruited personnel, including national personnel may be affected by any of these types of internal conflict differently than international personnel, and your description should be written in a way to later identify specific threats that may impact national and international staff differently.

Forces would be appropriate.

7. **Threat Groups/Actors.** This section is used to describe all groups and organizations which threaten instability and / or the control of the legitimate government in the SRM Area. They could be internal and/or external to the country and be comprised of citizens of the host nation or of other countries, or even armed forces of other countries. These groups could be linked to global or regional threat groups or may be specific only to the SRM Area. This section is about organized groups and includes terrorist groups, criminal groups, armed tribal militias and the like. These should be described in terms of their affiliations, leadership, size, agenda, capacity, training, geographic distribution, funding, international support, acceptance by local populations, and activities to date. It is important to note how these groups view the UN, and how have they affected UN security in the past.
8. **UN Mandate.** As applicable, describe any Security Council Mandate in place in the SRM Area and/or the strategic priorities of the Country Team. This must be done in the broadest of terms as a full Programme Assessment is part of the SRM Process. This section describes how this mandate and/or strategic priorities potentially affect the security situation and the security of the UN in the SRM Area. How is the UN mandate viewed by all parties? Have UN actions created problems in the past? Consider the perceptions of the local population and how they may react to the UN mandate. How could these past problems continue to affect security?

SRM Tool and Situational Analysis

Tip: If the SRM area is a peacekeeping mission, remember to describe what the role of the United Nations is in keeping parties to the civil war apart. Has this resulted in actions against Members of the Country Team, and from which side of the conflict?

An example of the SRM Tool is depicted below. The main headings of the Situational Analysis are provided in the form of tabs under which all of the subheadings are to be completed. Once again, in order to use this tool effectively, all of the descriptions under Situational Analysis must be kept as concise as possible.

UNDSS Security risk management e-Tool

Step 2: Situational Analysis

SRM area: **Congo, Democratic Republic of / Goma "CHANGE in PROGRESS"**
 Period from: **01-Nov-2015** to: **30-Nov-2015**

Political	Economic	Social	Environmental
Infrastructure	Country Security Forces	UN Mandate	Threat group/actors

Add description here (max 3800 char.)

Goma has been primarily affected by the large-scale political crisis for the last two years aimed at changing the long standing political regime. It is mainly in large scale demonstrations and civil unrest. Additionally the western region remains affected by armed clashes perpetrated by anti-government forces. In the eastern region, Al-Qaeda in the Four Sisters (AQFS), the local Al-Qaeda affiliate, continues to establish itself in the area. The term "Four Sisters" refers to the Four Sisters mountain range in the east on the border with Feydestan. The total number of security incidents reached their highest level for the year 2015 during which intensive demonstrations and localized armed incidents occurred in the context of the political crisis. However, the number notably decreased in November and December following the signing and initial implementation of the DPA led peace initiative.

Figure 4: Computer Tool – Situational Analysis

Step 3: Programme Assessment



STEP 3: Programme Assessment

The Conceptual Overview of the SRM process highlighted that SRM is a way to support programme delivery for the UN system by reducing risks to an acceptable level. Managers set goals and they manage people, resources and risk in order to achieve those goals. Managers also establish priorities among those goals.

To help the UN achieve its goals, it is necessary to understand those goals and the programmes it intends to implement. This is an ongoing process and is formally identified in UN system common planning documents such as the UN Development Assistance Framework (UNDAF), Humanitarian Response Plan (HRP) or Mission Concept⁹ etc. The process in the SRM by which the results and activities that the UN system needs to achieve to meet the goals is formally identified is the Programme Assessment. For SRM to “enable” the UN to deliver programme activities at an acceptable level of risk, there must be clarity about the programmes that are to be delivered.

As SRM depends on understanding and dealing with our vulnerability to threats, part of that understanding involves how programmes operate and how those operations may create exposure to threats.

Key Definition

Programme Assessment: A process by which the security professional formally comprehends the programme requirements of UNSMS Organizations.

Exposure

A question of whether staff may be subjected to a threat. It is generally a question of presence in an area where a threat exists and/or a question of whether the goals of a UN organization is in opposition to threat actor’s aims.

Therefore, assessing programmes is an ongoing activity of all UN staff with a security responsibility, led by the Security Professionals. It is not a one off activity of collecting information.

This stage in SRM, the Programme Assessment is a process by which the security professionals formally illustrates their comprehension of the programme requirements of UNSMS Organizations and highlights those programmes that may be *exposed to different threats or similar threats to different degree*. This is done through the collection and collation of strategic information provided by these organizations about their programmes as well as analysis to generate an understanding of common and exceptional exposure to threats. This should be completed in close collaboration with programme personnel at all levels.

The output of the programme assessment will be the recording of strategic goals and priorities of the UN as general information and recording programmes that have specific exposures to threats as specific information.

Two Parts to the Programme Assessment

There are two parts to the programme assessment; the “General” and the “Specific”. Where there are commonalities of exposure to threat, either through the type, acceptance or location of programmes, they have a common threat and their risk can then be assessed together. These commonalities are understood and represented through the understanding and recording of General information on UN programmes. Where there is a

⁹ DPA Missions may have a different planning document depending on the context of the mission.

programme or set of programmes that are relevant outliers or relevant exceptions from the General information then they potentially have different or additional threats and/or their risk, when assessed, may also be different. Therefore they need to be highlighted and identified with specific programme information.

The key information requirements in the Programme Assessment that must be made available to the security professional and used in the SRM process is therefore divided into two main sections:

General Information

General Information on the common goals and outcomes of the UNSMS organizations and their specific roles in conducting the programmes to achieve those goals is contained within UN planning documents such as the UNDAF, HRP or Mission Concept. However, reading and understanding these documents does not replace the depth of knowledge gained through attendance at UN Country Team, Humanitarian Country Team and planning meetings.

Through an understanding of these strategic planning documents of the General information will be used to identify the exposure implications to UN personnel, premises and assets from the intent of the UN operations. Programmes associated with the same goals and intents will generally assume similar profiles. For example if there are only development programmes running in the SRM area then it is likely that most UN programmes have a similar exposure in terms of the profile. If there are political programmes supporting the government in place and humanitarian programmes delivering assistance to those in need, it is likely that these different types of programmes have different exposures to similar threats.

At this stage of the SRM process it is only necessary physically to record the overview and key priorities of the general information on strategic planning documents. However, security advisers needs to consider how the UN strategies and common goals will influence the determination of threats once they get to the specific threat assessment.

Specific Information

Specific Information is required for UN activities and programmes that through their method of delivery, profile or geographical location are exposed to different threats or exposed to similar threats to a different degree. Put another way, Specific information will be used to provide increased granularity to the analysis of the exposure of individual programmes and this is best illustrated by examples:

- Exposure through Activity – In a country the majority of organizations may be carrying out humanitarian operations that are perceived to be neutral and impartial. There may also be a human rights office that while being equally neutral and impartial, is required to highlight human rights failures and this may be perceived differently. This is a different exposure.


- Exposure through Delivery Methods – The majority of organizations in an area may be delivering their programmes through implementing partners with monitoring carried out by national personnel. One agency, due to the capacities available, may need to deploy international staff in multiple field offices. These have different exposures.
- Exposure through Delivery Time – Using the above example, the majority of organizations may need to travel to an area to carry out programme monitoring irregularly, but at least once a quarter. Another agency may need to travel to the area on a daily basis. These have different exposures.
- Exposure through Delivery Locations – There may be a single organization with office(s) geographically separate from or more numerous than other organizations. This is a different exposure. Mapping of programme offices and operations is the best way to visualize this analysis.

The responsibility for identifying which UN activities have different exposures to threats does not lie with one individual or role; rather it is an ongoing consultative process between the Agency Representatives and Security Advisers to determine which activities and programmes need to be considered individually.

Once programmes have been identified as requiring specific consideration they need to be recorded with the following information for each programme:

- **What** – A list of the actions that involve UN personnel and how they will be implemented.
- **Who** – What category of UN personnel are involved (e.g. International? Locally recruited?) and in what way (e.g. resident in the area or on mission?).
- **When** – The frequency (daily, weekly or monthly) at which the activities will be conducted. In the event that the SRM is being conducted for a single, one-off activity, the exact date and times should be used.
- **Where** – Where within the SRM Area specifically are the activities focused?

There is no restriction on how many programmes can be listed and a Security Adviser may choose to list every programme being delivered in an SRM area. However, it should be noted that the only requirement for an effective SRM process is that the programmes identified as potentially having different exposures to the threats are recorded.



Security risk management e-Tool

← Back
Step 3: Programme Assessment
Next →

SRM area: **Yemen / Sana'a** ? Help
 Period from: **05-Nov-2015** to: **04-May-2016**


Development(UNDAF)
 Add description here (max 4000 char.)

Humanitarian(SRP)
 Add description here (max 4000 char.)

STRATEGIC OBJECTIVES
 The humanitarian response will be guided by the following strategic objectives and actions:
 1. Provide life saving assistance to people affected by conflict
 • Provide mass casualty management and life saving health care (including for malnutrition) and support referral

Mission
 Add description here (max 4000 char.)

Agency	Title	Nat	Int	City (nearest)	
WHO	vaccination campaign in local schools	1	2	Not set	Add New Delete
WHO	vaccination in Erbil schools	2	3	Kunduz	Delete
UNDP	Good Governance	17	2	Sana'a	Delete
DPA	Good Offices of Special Envoy to Secretary General	1	5	Sana'a	Delete



Security risk management e-Tool

← Back
Add new program
Save

Agency
 Please select agency.
 -- Select --

Title
 Add title here (max 100 char.)

Description
 Add description here (max 2000 char.)

Location
 Add location here (max 500 char.)

No. of national s/m (who is implementing the program)

No. of international s/m

Nearest city

Figure 5: Computer Tool – Programme Assessment

Step 4: Threat Assessment



STEP 4: Threat Assessment

The Threat Assessment is the process by which one identifies and assesses those actors and actions in the geographical area that may potentially cause harm to the United Nations system. Using the threat-related points generated during the Programme Assessment, it is necessary, in conjunction with the Security Cell, to list events that may block success (i.e., threats). In the UNSMS context, a security professional, and especially security analysts if available, are the key players in the threat assessment process to guarantee that senior managers get the best information on which to base their decisions.

There are two phases of Threat Assessment in the SRM process. The first, the General Threat Assessment, assesses various categories of threats in the SRM Area from the UN’s perspective. The second, the Specific Threat Assessment, evaluates the specific level of threat to the UN in the form of distinct undesirable events that could occur and affect the UN.

This Chapter will explain both levels of Threat Assessment and how they are conducted.

Remember:

Threat

The potential cause of harm in the environment caused by **deliberate** actions.

Hazard

The potential cause of harm in the environment caused by **non-deliberate** actions.

PART I: General Threat Assessment

The aim of the General Threat Assessment is to provide an objective description of the prevailing security threats and hazards in the environment of the SRM Area.

To ease understanding and discussion, the General Threat Assessment is broken down into four **Threat** categories as follows For the purpose of UNSMS security policies:

Armed Conflict – protracted confrontation involving military hostilities conducted by force of arms between parties to the conflict involving one or more governmental forces and/or formed non-governmental armed groups that take place within the territory of a state or between two or more states.

Terrorism - an act involving (destructive) physical violence intended to cause damage to person(s) and/or public or private infrastructure, when the purpose of such act, by its nature or context, is to intimidate or to compel a state, population or organization to undertake or to abstain from undertaking any specific actions.

Crime - an act that is forbidden by a public law and that makes the offender liable to punishment by that law, including violent crime, when an offender uses or threatens force upon a victim, in which the violent act can be both, the objective as well as the means to an end.

Civil unrest - (also known as civil disorder or civil strife) broadly refers to one or more forms of agitation or protest caused by a group of people involving a disruption of social order or normal daily life activities. The protest can be peaceful or involve violence, and can

take the form of legal or illegal actions which include, but are not limited to: demonstrations, strikes, sit-ins and other forms of obstructions, property damages, sabotage, petitions, riots, boycott, and rebellions. It can be local or widespread, and escalate into general chaos. It often seeks to give visibility to alleged human rights violations or major socio-political or socio-economic problems and/or to advocate for a change in policy or government structure.

Each of the four **threat** categories is assessed on three variables on a 1-5 scale:

- **Intent** The motivation or disposition of a threat actor to cause the threat event as described
- **Capability** The capacity or ability of threat actors to cause the threat event as described.
- **Inhibiting Context** (non-UN factors in the geographical area which inhibit Intent, Capability or both)

Examining threats in this manner provides a common basis to describe each threat according to its *willingness to do harm*, its *ability to do harm* and the *aspects of the environment*, such as the norms of the community or the capacity of the host government or local authorities, which may *constrain or encourage a threat*. In this way, Intent and Capability are “drivers” in the threat and Inhibiting Context is a “restrainer” of the threat.

As with the threat variables above, History and Severity/Intensity are “drivers” in the hazard and Warning/Preparedness is a “restrainer” of the hazard.

To ensure reliability (i.e., that the assessment will achieve similar results when different people conduct the assessment), each threat category (Armed Conflict, Terrorism, Crime, Civil Unrest) has distinct descriptors for subjectively rating each of the three variables (Intent, Capability and Inhibiting Context). Below are the ranking matrices for each of the five Categories in the General Threat Assessment.

Armed Conflict

	Intent	Capability	Inhibiting Context
1	No intention to use armed / military force	No or very limited presence of hostile military-type capability (no or very limited military-type weapons, training, etc.)	Strong deterrent against initiating conflict
2	Indications that military force is seen as an option or statements threatening attack but political solution still possible	Small arms/Automatic (light) Weapons (AK47, mortars, RPG) but minimal military-type training/experience and loosely organized	Pressure/other incentives/agreements against hostilities
3	Clear statements on imminent attack and peaceful options exhausted	Organized and structured forces with increased mobility and/or standoff/indirect (medium) weapon capability	Peace talks or unstable peace/cease-fire agreement
4	Isolated / Limited / Sporadic armed conflict occurring	Organized and structured forces w/ HW deployed and/or large numbers of forces and intensified military operations	No restraint/pressure to prevent continuation or outbreak of conflict
5	Full-scale armed conflict occurring	Organized structured forces with HW deployed or large number of forces fully engaged	Armed conflict already occurring in area

Terrorism

	Intent	Capability	Inhibiting Context
1	Intent to use terrorism against the UN acknowledged worldwide	No known terrorist capability (threats and harassment only tactic)	Security forces effective
2	Intent to use terrorism and/or small-scale attacks	Limited to small-scale/individual basic operations	Security effective and/or social support of cause
3	Wide-spread small-scale attacks on local infrastructure	Some isolated but coordinated operations which produce limited effects	Security moderately effective and/or active assistance to terror cells in some areas
4	Sustained or large-scale attacks and/or statements or actions demonstrating intent to target UN	Demonstrated capacity in wider-range and varied terror attacks	Security forces challenged to prevent terrorist activities
5	A group has already attacked the UN and is still operational in the area	Demonstrated ability in all terror tactics to produce mass destruction and/or casualties (complex attacks)	Minimal ability to deter terrorist attacks. Terrorists have safe havens

Crime

	Intent	Capability	Inhibiting Context
1	Property crime, seldom violent	Generally lone, unarmed criminals	Police/criminal justice system effective and crime is socially unacceptable
2	Opportunistic crime against individuals, seldom violent	Generally lone criminals, sometimes armed	Crime is not socially acceptable; police/CJ system not fully effective
3	Violent crimes focus on relatively affluent elements of the community	Lone, armed criminals and/or unarmed criminals operating in small teams	No major social constraints on crime; police/CJ system stressed
4	Wide-spread violent crimes	Armed criminals operating in small teams	Police/CJ system significantly challenged

5	Prevalence of violence w/frequent fatalities and/or focus on the UN	Organized, armed criminal gangs	Minimal social or Police/CJ controls on criminal activity
---	---	---------------------------------	---

Civil Unrest

	Intent	Capability	Inhibiting Context
1	Peaceful crowds only	<100 people	Effective crowd control or crowd self-controlled
2	Some crowds become disruptive	<500 people	Crowd control not fully effective
3	Crowds become violent/localized riots	<1000 people	Crowd control mechanisms stressed (numbers, equipment, etc.)
4	Extensive/wide-spread violent crowds/riots (UN possible target)	<5000 people	Challenged crowd control mechanism or some possibly to allow anti-UN protests
5	Violent crowds/riots targeting UN	5000+ people	Minimal crowd control mechanisms

Hazards

	History	Intensity/Severity	Warning/Preparedness
1	Not prone to hazard events	Limited	Effective warning and preparedness systems in place
2	Hazard events occur occasionally	Moderate	Partial/limited warning and/or preparedness systems in place
3	Hazard events occur frequently	Severe	Warning and/or preparedness systems in place not fully effective
4	Prone to predictable hazard events and/or hazard event imminent	Devastating	Warning and/or preparedness systems are untested or unknown
5	Prone to sudden onset hazard events	Multiple and devastating	No warning and/or preparedness systems in place

The General Threat Assessment requires the choice of one descriptor for each variable in each threat/hazard category. If it is difficult to choose between two descriptors, the SRM Tool allows the user to choose a “half point” between the two (e.g., 2.5 between 2 and 3). The scores for the three choices are added up to give a threat score for each Category. Here is an example using the Armed Conflict Category:

Armed Conflict

It is not sufficient to do this assessment using only generic information. If scores in the 4 and 5 range for Intent and Capability are selected for example, specific information would be required.

	Intent	Capability	Inhibiting Context
1	No intention to use armed / military force	No or very limited presence of hostile military-type capability (no or very limited military-type weapons, training, etc.)	Strong deterrent against initiating conflict
2	Indications that military force is seen as an option or statements threatening attack but political solution still possible	Small arms/Automatic (light) Weapons (AK47, mortars, RPG) but minimal military-type training/experience and loosely organized	Pressure/other incentives/agreements against hostilities
3	Clear statements on imminent attack and peaceful options exhausted	Organized and structured forces with increased mobility and/or standoff/indirect (medium) weapon capability	Peace talks or unstable peace/cease-fire agreement
4	Isolated / Limited / Sporadic armed conflict occurring	Organized and structured forces w/ HW deployed and/or large numbers of forces and intensified military operations	No restraint/pressure to prevent continuation or outbreak of conflict
5	Full-scale armed conflict occurring	Organized structured forces with HW deployed or large number of forces fully engaged	Armed conflict already occurring in area

In this example, the Intent score is **2**, the Capability score is **3** and the Inhibiting Context score is **1**. The total threat score for Armed Conflict is **6**.

VALIDITY CHECK

At this stage, it is important for the security professional to conduct a “validity check” by comparing the numerical rating made for each variable with the numbers given to other variables and for the same variable in different locations to see if there are any anomalies that render the overall assessment invalid. Simple questions like, “Does it make sense that the Capability rating for Armed Conflict in this SRM Area is higher than the Capability rating for Armed Conflict in that SRM Area?” help ensure consistency throughout assessments.

After the validity check, the total threat score is compared with the range of scores in the table below to get a Threat Rating. For the example above, with a threat score of 6, the Threat Rating for Armed Conflict in this SRM Area would be Low (between 5 and 7) (*Note: in the actual SRM Tool, the addition of the scores for Intent, Capability and Inhibiting Context and the ranking of this score within the appropriate Threat Rating is done automatically.*)

Threat Score Range	Threat Rating
3 to <5	Minimal
5 to <7	Low
7 to <9	Moderate
9 to <11	Substantial
11 to <13	High
13 to 15	Extreme

The results of the General Threat Assessment will be displayed as a graph to visually highlight which General Threat category rating is the highest. The graph can also display one threat category across multiple SRM areas, or multiple threat categories for just one SRM area.

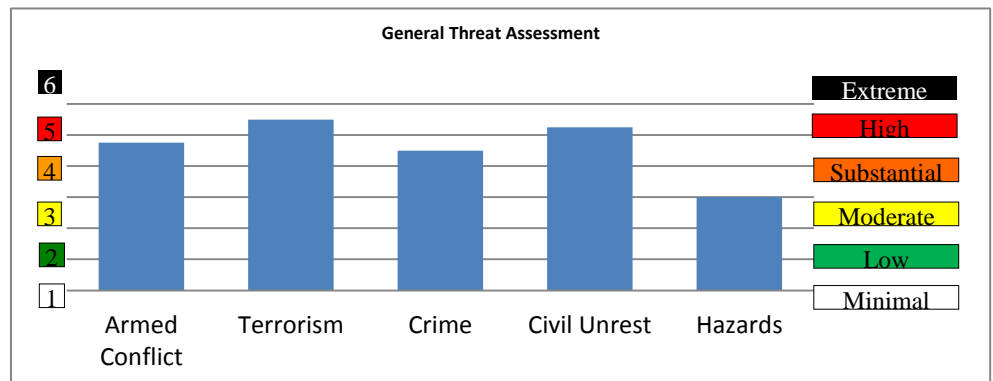


Figure 6: Output of the General Threat Assessment

At this point we must highlight again what is emphasized in the Introduction to this Manual: of prime importance is familiarity and knowledge of the security situation in the area in which you wish to apply the SRM process. Each choice made in the General Threat Assessment must be based on credible facts, and the facts must be relative to the SRM Area for which this assessment applies (choices should also reflect threat-related information gathered in the Situation Analysis). Conducting the General Threat Assessment using this methodology without a detailed understanding of the security environment, or using incorrect or erroneous information, will corrupt all the remaining steps of the SRM Process.

Annex D has detailed additional comments on all the threat descriptors. The descriptors and their supplemental information will also be available when using the SRM Tool.

It is important to note that the General Threat Assessment is not a predictive tool. It is based on current and historical information, but does not try to anticipate future changes in the threat. It describes each category of threat and hazard as they exist *now* in the SRM Area. It does so by selecting the most appropriate descriptor for the variable being assessed.

In addition to providing threat scores and threat ratings for each category, the General Threat Assessment can also produce a Security Level for that SRM Area. See Annex D for a description of how this process works.

PART II: Specific threats and event descriptions

Specific Threat Assessment

The Specific Threat Assessment is the stage of the SRM process that identifies the specific threats to the United Nations for the SRM Area and provides a structured assessment of these threats in a similar way as the General Threat Assessment. Unlike the General Threat Assessment – which looks at the overall threat environment in the SRM area – the Specific Threat Assessment identifies the precise threats to the United Nations in that area.

Event Descriptions

Specific

Key Definitions

Event Description: Clear description of a harmful event that the SRA will examine and must include the effect on the Organization.

The concept outlines that vulnerability to a threat may eventually manifest itself in the occurrence of undesirable events, and that risk is assessed as the combination of the likelihood of an undesirable event occurring and the impact would have if it were to occur. Therefore, to conduct a Specific Threat Assessment, it is necessary to generate an Event Description linked to the specific threat. An **Event Description** is:

The clear description of a harmful event (that involves harm to personnel, programmes or assets) that the SRA will examine, and must include the negative **effect on the UN**.

It is important to see that an Event is not the same as a Threat. We can do a Risk Assessment (Impact and Likelihood) on an Event but not on a Threat.

The identification of potential event descriptions to the UN in the SRM Area must be based on the security environment as indicated in the Situational Analysis, Step 2, as well as actual security incidents which have occurred in the SRM Area. It is important to collect as much specific information as possible, as generic information is of lesser value in determining event descriptions. The incidents analyzed may have been directed at the UN or not, as understanding the entire threat environment is required to understand specific threats. Sources of information to complete this section of the SRM process could be UN security incident databases; provided by host nation security forces; provided by INGO/NGO partners; where applicable, provided by international armed forces in the SRM area; DSS and other UN HQ entities; third party member states; open source information (e.g., think tanks and other academic institutions); neighboring UN missions or country teams; and, most importantly the country team and other UN actors in the SRM area itself.

The incident data is however not enough; it has to be analyzed to determine trends and patterns in order to fully justify the identification of a potential event description to the UN in the SRM area. This will require a certain degree of analysis, the creation of charts and graphs, and mapping the incidents so as to extract the actual meaning of incidents that have occurred before. The “So What” principle must be applied when considering factual information in order to determine the real security implications of these incidents. This will allow a more credible determination of potential, specific events.

An effective Event Description will provide security professionals with clear parameters for examination. Event Descriptions should include references to *Who* may perpetrate the event, *What* the specific event may be, *When* the event may take place, *Where* the specific event may occur within the SRM Area, and/or *How* the specific event is envisaged. Note that the *Why* components are not generally required as it is generally irrelevant for the purposes of event identification. Event Descriptions do not necessarily require all of these components but should include as many as realistically necessary to inform the problem.

The following are two examples of Event Descriptions:

“Kidnapping targeting UN International staff for criminal ransom by non-state actors in Area 1”

[What] [UN focus] [Direct] [Who] [Where]

“UN vehicle targeted and hit by IED along road X to Field Office Y”

[UN Focus] [Direct] [What] [Where]

These Event Descriptions provide sufficient information to narrow down the parameters involved and will allow for a more accurate assessment of the event than a general threat statement such as “Kidnapping”.

The table below shows an example of how a list of event descriptions is generated. Note that each Specific Threat has a “worst case” and “least-worst case” event description. The purpose of having two event descriptors with different outcomes is important to ensure the security practitioners understand various possible outcomes.

Key Definitions

For the Specific Threat Assessment

Intent: The motivation or disposition of a threat actor to cause the threat event as described.

Capability: The capacity or ability of threat actors to cause the threat event as described.

Inhibiting Context: How permissive the context is for the threat actors to cause the event as described.

Category	Specific Threat	Event Descriptions
1. Armed Conflict	Armed Incident – UN Targeted	1. UN office damaged by mortar fire 2. UN personnel killed by mortar fire
	groupsArmed Incident - Incidental	3. UN personnel injured when caught in cross-fire 4. UN personnel killed in cross-fire
2. Terrorism	groupsArmed Incident - Incidental	5. UN office damaged by VBIED targeting government
	Armed Incident – UN Targeted	6. UN personnel killed in VBIED attack on UN office 7. Complex attack on the UN office (no injuries)
3. Crime	Armed Incident – UN Targeted	8. UN Personnel killed in compound during complex attack 9. UN vehicle stolen at gun point
	Robbery	10. UN personnel shot during car-jacking
	Theft	11. Official computer laptop stolen from UN office 12. Large amount of cash stolen from UN office
4. Civil Unrest	Public Gathering- Non Violent	13. Peaceful demonstration at UN office
	Public Gathering- Violent	14. Violent, anti- UN demonstration at UN office
	Public Gathering- Non Violent	15. Religious rioting blocks roads near the UN office
	Public Gathering- Violent	16. Religious rioting attacks UN offices and kills personnel

Event Descriptions should also reflect whether events result from a direct or indirect threat to the UN. *Direct* threats are those specific to the UN. Either a particular belligerent group or individual has stated the intent to do harm to the UN, or recent history has shown that the UN is the target of such a threat. This could include a deliberate attack on a UN office or vehicle, a public demonstration directed at a UN location or the kidnapping of a UN personnel member for political or financial purposes. *Indirect* threats are those which may affect the UN negatively in a wrong-place-wrong time scenario, through collateral damage, by association with the actual target, or where the UN is in the way. This could include personnel caught in crossfire between armed elements, or a public demonstration that damages a UN vehicle that happens to be near the crowd. It is important to note that the differentiation between direct and indirect can sometimes have a very significant effect on the eventual outcome of the risk assessment and so careful consideration, and notation, is required for this component of the Specific Threat Assessment. Both direct and indirect threats can be further subdivided into those which

Drafters of RMAs are encouraged to consult the Security Analysis Handbook for greater detail on types of information and threats. The Handbook is available in the library on UNSMIN.

are “known” (where statements of intent to harm the UN has been made or it has happened before), or, “assessed” (where although no intent has been stated, the analyst assesses that the threat exists).

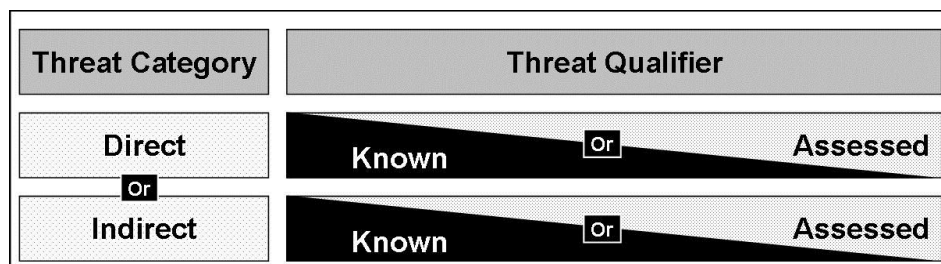


Figure XX

The importance of clear and detailed Event Description cannot be overstated. The identification and recording of these Event Descriptions in the Specific Threat Assessment will effectively drive the rest of the SRM process. Well-defined and realistic Event Descriptions will produce a valid and helpful SRA, but vague or misleading Event Descriptions will produce a poor assessment of risks facing the UN.

Note Remember from the Programme Assessment we identified where there are programmes being delivered that are outliers from the “normal” operations of the UN. Where certain programmes or agencies may be exposed to threat or have a different profile they require specific event descriptions. *This is reflected in the event descriptions and could look like the examples below:*

Key Definitions

For the Specific Threat Assessment

Intent: The motivation or disposition of a threat actor to cause the threat event as described.

Capability: The capacity or ability of threat actors to cause the threat event as described.

Inhibiting Context: How permissive the context is for the threat actors to cause the event as described.

Category	Specific Threat	Event Descriptions
1. Armed Conflict	1. Armed Incident – UN Targeted	1. UN office damaged by mortar fire 2. UN personnel killed by mortar fire
	2. Armed Incident - Incidental	3. DPKO personnel injured when caught in cross-fire 4. DPKO personnel killed in cross-fire
2. Terrorism	1. Armed Incident – UN Targeted	5. UN office damaged by VBIED targeting government 6. UN personnel killed in VBIED attack on UN office
	Armed Incident – UN Targeted	7. Complex attack on the UN office (no injuries) 8. UN Personnel killed in compound during complex attack
3. Crime	Robbery	9. UN vehicle stolen at gun point 10. UN personnel shot during car-jacking
	Theft	11. Official computer laptop stolen from UN office 12. Large amount of cash stolen from UN office
	Public Gathering- Non Violent	13. Peaceful demonstration at UNDP Country office 14. Peaceful demonstration at UN Agencies office
4. Civil Unrest	Public Gathering - Violent	15. Violent, anti-UN demonstration at UN office
	Public Gathering- Non Violent	16. Religious rioting blocks roads near the UN office
	Public Gathering - Violent	17. Religious rioting attacks UN offices and kills personnel

In the example above the programme assessment identified:

- Only DPKO personnel are operating in the areas of active conflict and so in the event description it is made clear that this only affects DPKO personnel.
- The UNDP country office is a higher profile location than other UN

offices and so there are two event descriptions (one for UNDP office and one for the other offices) that will allow the risk assessment to consider the differences in the risk and allow security decision makers to take nuanced and appropriate risk management decisions.

Threat Assessment

Once the Specific Threats are identified and Event Descriptions have been fully laid out, the next step is the actual assessment of each event. Just like the General Threat Assessment, the Specific Threat Assessment evaluates each event on three variables: Intent (of the threat actor¹⁰), Capability (of the threat actor), and Inhibiting Context (of the environment in which the threat occurs) in regards to the event **as described** in the Event Description.

- **Intent** – This is defined as “the motivation or disposition of a threat actor to cause the threat event as described” and refers to the mental orientation of the threat actor towards the target. In cases of Direct Threats, security professionals are able to assess Intent against pre-set qualifiers using existing knowledge (e.g. measuring intent of kidnapping based on publicly expressed design and/or past incidents). For Indirect Threats, security professionals will have to utilize existing knowledge of the general situation. For example there may be Indirect Threats where threat actors have stated intent to do harm to non-UN organizations, such as Government Ministries, and while this threat is not directed at the UN, given UN personnel may work in these Government Ministries, it must be considered as an Indirect Threat; or, recent trends observed in the ongoing conflict between the rebels and the Government indicate that the fighting is moving closer to two IDP camps administered by UNHCR. Collateral damage from inaccurate rebel or government artillery and rocket fire could present an Indirect Threat to the UN.
- **Capability** – This is defined as “The capacity or ability of threat actors to cause the threat event as described.” This component refers to the physical ability of the threat originator to carry out the threat event *if it so desired*. Capability combines elements of knowledge, skill and training; financial resources; human resources; planning and coordination; and logistic resources to execute a particular course of action. Typically both resources and knowledge are required; one without the other means that there is no capability. Capability must be assessed for the timeframe of this risk assessment for it to be rated. For example, an extremist organization may be very capable, but if the fighters and equipment are not deployed in the geographical area under consideration, for the purposes of the threat assessment, the capability should be rated low because the capability is not “in the environment”.

¹⁰ “Threat actor” could refer to Direct Threats (e.g. demonstrations against the UN, terrorism against the UN, targeting of small arms against the UN, etc.) or it could refer to Indirect Threats (e.g. UN caught in crossfire between armed groups, landmines and other UXO, etc.).

- **Inhibiting Context** – This is defined as “how permissive the context is for the threat actors to cause the event **as described**” and refers to the external (i.e. non-UN) environment in which the threat exists and the degree to which the environment is hostile or permissive to the threat and/or the threat originator. This component can be very broad, and care must be taken to not overreach. It may include elements such as the effectiveness of local law enforcement, or the general disposition of a given society towards that particular threat or threat actor.

As with the General Threat Assessment, the Specific Threat Assessment requires that one descriptor is chosen for each variable from the 1-5 scale, this time focusing on the event as described in the Event Description and using the table below. If it is difficult to choose between two descriptors, the SRM Tool allows the user to choose a “half point” between the two (e.g., 2.5 between 2 and 3).

	Intent	Capability	Inhibiting Context
1	No intention to execute the event against the UN	Evidence that no capability to execute the event	Very non-permissive environment to execute the event
2	Only expressed intention or evidence that event type is seen as an option	Minimal/limited capability to execute the event	Environment generally non-permissive to the event
3	Full demonstrated intent to execute the event against the UN but w/ only preliminary planning	Moderate capability to execute the event	Environment challenged to inhibit the event
4	Actors have already executed the event (not against the UN) or evidence of advanced planning and preparation against the UN	Substantial capability to execute the event	Environment generally permissive to the event
5	Full demonstrated intent to execute the event against the UN (have already executed event against the UN)	Full demonstrated capability to execute the event	Very permissive environment to execute the event

The scores for the three choices are added to give an overall Threat Score for the event. Each event, therefore, will get a Threat Score and a Threat Rating, exactly like the general threat categories in the General Threat Assessment.

The example below gives a Threat Score of 12 (4+5+3), and based on the same score distribution, the Threat Rating for the event is High.

	Intent	Capability	Inhibiting Context
1	No intention to execute the event against the UN	Evidence that no capability to execute the event	Very non-permissive environment to execute the event
2	Only expressed intention or evidence that event type is seen as an option	Minimal/limited capability to execute the event	Environment generally non-permissive to the event
3	Full demonstrated intent to execute the event against the UN but w/ only preliminary planning	Moderate capability to execute the event	Environment challenged to inhibit the event

Important!

Managers are reminded that decisions are **not** made on the basis of “threat” but on “risk”. It is entirely possible to be confronted with a high threat that poses low risk to the UN in a given area. The purpose of the overall threat score is simply to provide a preliminary and relative view of threats in an area. Only after completing the next step in the SRM process – the Risk Analysis – will risk managers have sufficient information to begin planning Security Risk Management strategies.

4	<i>Actors have already executed the event (not against the UN) or evidence of advanced planning and preparation against the UN</i>	<i>Substantial capability to the event</i>	<i>Environment generally permissive to the event</i>
5	<i>Full demonstrated intent to execute the event against the UN (have already executed event against the UN)</i>	<i>Full demonstrated capability to execute the event</i>	<i>Very permissive environment to execute the event</i>

Threat Score Range	Threat Rating
3 to <5	Minimal
5 to <7	Low
7 to <9	Moderate
9 to <11	Substantial
11 to <13	High
13 to 15	Extreme

It is imperative that security professionals fully consider each component of each Event Description within their Specific Threat Assessment and gauge their assessments as objectively, and comprehensively, as possible. It is equally imperative that these assessments are based on factually based judgments and not on supposition, hearsay or conjecture. Choices made here should also reflect threat-related information gathered in the Programme Assessment.

At no time should the descriptions be chosen in order to achieve a desired Threat Rating. Any attempt to “retro fit” the General or Specific Threat Assessment will corrupt the whole SRM process. Considering that security decisions should never be made based on threat, there is absolutely no reason to manipulate the result of any threat assessment and too many reasons not to.

Once each Event Description is assessed by evaluating the three components of intent, capability and inhibiting context, an overall Threat Score will be auto-generated and retained in the online system. The overall Threat Scores will then be used further in the SRM process thus:

- Security professionals will have an overview of the overall threat scores for all events. This will give them a clear ranking of the severity of each threat in the geographical area relative to the others and, if needs be, relative to other threats in other areas of UN operation.
- The overall threat scores will also be stored by the system for the next phase of the SRM process – the Security Risk Analysis.

Step 4, part 1: General Threat Assessment

SRM area: **Yemen / Sana'a**
 Period from: **05-Nov-2015** to: **04-May-2016**

Armed conflict | Terrorism | Crime | Civil unrest | Hazards

Intent:	Capability:	Inhibiting context:
1 <input type="radio"/> No intention to use armed/military force <input type="radio"/> In between	1 <input type="radio"/> No or very limited presence of hostile military-type capability (no or very limited military-type weapons, training, etc.) <input type="radio"/> In between	1 <input type="radio"/> Strong deterrent against initiating conflict <input type="radio"/> In between
2 <input type="radio"/> Indications that military force is seen as an option or statements threatening attack but political solution still possible <input type="radio"/> In between	2 <input type="radio"/> Small arms/Automatic (light) Weapons (AK47, mortars, RPG) but minimal military-type training/experience and loosely organized <input type="radio"/> In between	2 <input type="radio"/> Pressure/other incentives/agreements against hostilities <input type="radio"/> In between
3 <input type="radio"/> Clear statements on imminent attack and peaceful options exhausted <input type="radio"/> In between	3 <input type="radio"/> Organized and structured forces with increased mobility and/or standoff/indirect (medium) weapon capability <input type="radio"/> In between	3 <input type="radio"/> Peace talks or unstable peace/cease fire agreement <input type="radio"/> In between
4 <input checked="" type="radio"/> Isolated armed conflict occurring <input type="radio"/> In between	4 <input checked="" type="radio"/> Organized and structured forces w/ HW deployed and/or large numbers of forces and intensified military operations <input type="radio"/> In between	4 <input type="radio"/> No restraint/pressure to prevent continuation or outbreak of conflict <input checked="" type="radio"/> In between
5 <input type="radio"/> Full-Scale armed conflict occurring	5 <input type="radio"/> Organized structured forces w/ HW deployed or large number of forces fully engaged	5 <input type="radio"/> Armed conflict already occurring in area

Figure 4: Computer Tool – General Threat Assessment

Step 4, part 2: Specific Threat Assessment - Event description

SRM area: **Yemen / Sana'a**
 Period from: **05-Nov-2015** to: **04-May-2016**

General threat: **Armed Conflict** | Specific threat: **Armed incident - incidental** | D/I: **Direct** | **Add**

Add Event description here (max 1000 char.)

General threat	Specific threat	Event description	D/I
Armed Conflict	Armed incident - UN targeted:	Armed Attack on the Special Envoy to the Secretary General	Direct Delete
Armed Conflict	Armed incident - incidental	Stray rounds hit UN office in Unolocia due to continued armed clashes between the government and opposition tribes. No UN casualties.	Indirect Delete
Armed Conflict	Armed incident - incidental	UN personnel in UN premises in Unolocia injured by AQFS VBIED (car or motorcycle)	Indirect Delete
Terrorism	Armed incident - UN targeted:	Complex attack on UN Compound (all agencies less UN house)	Direct Delete
Terrorism	Armed incident - UN targeted:	Direct Attack on SGSE during movement	Direct Delete
Terrorism	Armed incident - incidental	UN personnel in UN housing in the eastern governates killed by AQFS VBIED (car or motorcycle)	Indirect Delete
Terrorism	Armed incident - UN targeted:	Use of chemical weapons against UN staff	Direct Delete
Crime	Robbery	UN personnel killed during vehicle highjacking in the Central Region	Direct Delete

Figure 5: Computer Tool – Specific Threats and Event Descriptions



Security risk management e-Tool

Step 4, part 2: Specific Threat Assessment

SRM area: **Yemen / Sana'a**
 Period from: **05-Nov-2015** to: **04-May-2016**

General threat	Specific threat	Event description	D/I	? Int	? Cap	? Cntx	Total	Descriptor
Armed Conflict	Armed incident – UN targeted:	Armed Attack on the Special Envoy to the Secretary General	Direct	4.0	3.5	3.0	10.5	Substantial
Armed Conflict	Armed incident – incidental	Stray rounds hit UN office in Unolocia due to continued armed clashes between the government and opposition tribes. No UN casualties.	Indirect	5.0	3.0	4.0	12	High
Armed Conflict	Armed incident – incidental	UN personnel in UN premises in Unolocia injured by AQFS VBIED (car or motorcycle)	Indirect	3.0	1.5	4.0	8.5	Moderate
Terrorism	Armed incident – UN targeted:	Complex attack on UN Compound (all agencies less UN house)	Direct	3.0	3.0	2.0	8	Moderate
Terrorism	Armed incident – UN targeted:	Direct Attack on SGSE during movement	Direct	4.0	3.5	4.0	11.5	High
Terrorism	Armed incident – incidental	UN personnel in UN housing in the eastern governates killed by AQFS VBIED (car or motorcycle)	Indirect	4.5	3.5	1.5	9.5	Substantial
Terrorism	Armed incident – UN targeted:	Use of chemical weapons against UN staff	Direct	3.0	4.0	2.0	9	Substantial
Crime	Robbery	UN personnel killed during vehicle highjacking in the Central Region	Direct	5.0	3.0	5.0	13	Extreme

Intention

1. No intention to execute the event against the UN
2. Only expressed intention or evidence that event type is seen as an option
3. Full demonstrated intent to execute the event against the UN but w/ only preliminary planning
4. Actors have already executed the event (not against the UN) or evidence of advanced planning and preparation against the UN
5. Full demonstrated intent to execute the event against the UN (have already executed event against the UN)

Capability

1. Evidence that no capability to execute the event
2. Minimal/limited capability to execute the event
3. Moderate capability to execute the event
4. Substantial capability to the event
5. Full demonstrated capability to execute the event

Inhibiting context

1. Very non-permissive environment to execute the event
2. Environment generally non-permissive to the event
3. Environment challenged to inhibit the event
4. Environment generally permissive to the event
5. Very permissive environment to execute the event

Figure 6: Computer Tool – Specific Threat Assessment

Step 5: Security Risk Assessment



STEP 5: Security Risk Assessment

Overview

Various aspects of the threat assessment will influence your judgment about both the likelihood and impact of a certain threat. To illustrate, we can use an example about armed crime.

If the threat assessment identifies a threat from large, well-armed criminal groups working in a city with poor lighting at night and a weak police force, then the likelihood of a successful attack may be high. If a criminal group is known to use weapons during armed robberies, and have a history of killing all witnesses, then the potential impact could be loss of life, so the risk associated with this group would be greater than if they did not have weapons and a history of using these.

A person's presence in an area of poor lighting, where the criminal group is known to operate, makes him or her vulnerable, and affects the risk assessment. The risk associated with an attack by even a small, unarmed criminal group will be higher if the target is not properly protected. A lack of ability to control the after-effects of a serious incident is also a form of vulnerability and needs to be examined. *The risk of someone dying after being shot in an armed robbery, for example, will increase if proper medical attention is not given to the victim.*

Only after you have identified all the major threats and established their corresponding risks, are you ready to make sound decisions on how to lower risks.

The Concept of Likelihood in the UNSMS

The determination of Likelihood has traditionally been one of the most difficult and ambiguous steps in the UNSMS SRM process. Cognitive bias and limited data available to risk managers have sometimes resulted in Likelihood assessments (and, therefore, risk assessments) that are inaccurate and, often, unhelpful.¹¹ Inflation of risk unnecessarily inhibits delivery of the programmes of UN organizations.

Determining Likelihood through scientific, quantitative methods is only possible with any degree of reliability in cases of events with large data sets. Using quantitative methods in most contexts in which the UN operates will very rarely produce valid results because the amount of data available is insufficient to construct valid models. The UNSMS SRM model recognizes that a purely mathematical approach, utilizing advanced statistical analysis and modeling is not always a realistic method in our context.

UN operations often deal with threats of a deliberate nature and it is

¹¹ The UNDSS SAPP course addresses these issues explicitly and there is a wealth of literature on cognitive psychology, bias and heuristics in mainstream academia. Risk professionals are encouraged to pursue these subjects in the course of their professional development.

Key Definitions**Likelihood:**

A rating (1-5 or Very Unlikely, Unlikely, Moderately Likely, Likely, Very Likely) of the assessed potential of an undesirable event affecting the UN.

Likelihood = **Threat** x **Prevention Vulnerability**

Likelihood = **Threat** (Intent + Capability + Inhibiting Context) x **Prevention Vulnerability**

important to acknowledge that just because something has never happened before (zero incidence) it doesn't mean it won't happen in the future. This is particularly the case for the threat of terrorism, where improbable disastrous events do sometimes transpire. These types of events are improbable as opposed to impossible. However, just because improbable events sometimes do take place does not mean that all improbable events therefore become probable. To avoid or to ignore this elemental consideration is to engage in faulty planning and decision-making.

Likelihood in the UNSMS SRM model is defined as “a rating of the assessed *potential* for a harmful event to effect the Organization.” And is measured on a scale of 1-5 or Very Unlikely, Unlikely, Moderately Likely, Likely, Very Likely.

In the UN SRM process, Likelihood of an event is a product of Threat and Vulnerability (i.e., Likelihood = Threat x Prevention Vulnerability).

[Remember that threat is a combination of Intent, Capability and Inhibiting Context and this was assessed in the previous step – the Specific Threat Assessment.]

The Likelihood score for an event is achieved by multiplying the Threat Score for the event (calculated in the Specific Threat Assessment step) by the 1-5 Prevention Vulnerability score (explained below).

This approach to Likelihood has been developed to reflect the “potential” of a deliberate event to occur by measuring both the changing threat (Intent, Capability, and Inhibiting Context) and our relative ability to prevent the event from occurring (Prevention Vulnerability)¹². Even though an event has never happened before, if the intent and capability are rising in a formerly permissive environment, and we've done nothing to prevent the event from occurring and affecting us, then the event is more likely to occur and affect us.

Prevention Vulnerability Assessment

As noted previously, Vulnerability is defined as “a weakness that can allow a threat or hazard to cause harm”. A Vulnerability Assessment is an assessment of the strengths and weaknesses of our security system – an assessment of whether the necessary security countermeasures are in place and effective (strength) or absent and/or ineffective (weakness).

At this stage it is important to remember that the SRM process divides vulnerability into two components – Prevention Vulnerability and Mitigation Vulnerability. Prevention Vulnerability deals with Likelihood while Mitigation Vulnerability deals with Impact (see below for more on Mitigation Vulnerability).

When discussing Likelihood, therefore, the following two definitions are

¹² The UNSMS differentiates between Prevention Vulnerability (vulnerabilities that influence the Likelihood of a threat from occurring) and Mitigation Vulnerabilities (vulnerabilities that influence the Impact of a threat when it occurs). Some vulnerabilities, of course, are both Prevention-related and Mitigation-related.

Key Definitions**Vulnerability:**

A weakness that can allow a threat or hazard to cause harm

Vulnerability Assessment:

An assessment of whether the necessary security countermeasures are in place (strength) or absent (weakness).

Vulnerability = **Prevention Vulnerability** (affecting Likelihood) + **Mitigation Vulnerability** (affecting Impact).

Prevention Vulnerability:

The absence of security countermeasures meant to lower the likelihood of the event occurring as described.

Prevention Vulnerability Assessment:

An assessment of the level to which the UN has implemented effective measures to lower the likelihood of the event occurring.

required:

- **Prevention Vulnerability:** inadequate security countermeasures meant to reduce the **Likelihood** of the event occurring as described.
- **Prevention Vulnerability Assessment:** An assessment of the degree to which the UN has implemented effective security countermeasures to lower the **Likelihood** of the event occurring.

The UNSMS SRM Process uses a 1-5 scale for Prevention Vulnerability:

1. Effective preventive risk management countermeasures/ procedures completely in place and consistently effective.
2. Effective preventive risk management countermeasures/procedures completely in place (but a weakness exists that could be exploited given substantial resources).
3. Preventive risk management countermeasures/procedures not completely in place OR not consistently effective.
4. Preventive risk management countermeasures/procedures not completely in place AND not consistently effective.
5. No effective preventative risk management countermeasures/procedures in place.

As with the determination of components for Specific Threats, the UNSMS SRM Manual cannot provide a comprehensive list of all descriptors and qualifiers for Prevention Vulnerability. Security professionals must ensure that they fully consider the multitude of variables in determining Prevention Vulnerability in an objective, realistic and evidentiary (i.e. fact-based) manner.

As with the Threat Assessment step above, it is important for the security professional to conduct a “validity check” by comparing the numerical rating made for Prevention Vulnerability for one event description with the rating given for other event descriptions to see if there are any anomalies that render the overall assessment inconsistent and/or invalid. Simple questions like, “Does it make sense that the Prevention Vulnerability rating for this event is lower than for this other event?” helps ensure consistency throughout assessments.

When making the Prevention Vulnerability assessment, security professionals must record what prevention measures are in place and how effective they are in order to lower the likelihood of the event. This information will be used to design recommendations for lowering likelihood/lowering prevention vulnerability later (see “Step 6: Security Risk Management Measures” below). It is important to note that in this step, security professionals reflect only on the measures currently in place and their effectiveness. There is space in the etool for the drafter to note specific comments relevant to each Event Description. For example, the drafter may note *untrained guards are in place* or *access control measures are in place and effectively implemented*. At this stage the drafter does NOT consider measures that are not in place.

The components of the Specific Threat Assessment – Intent, Capability and Inhibiting Context – are completed during the Specific Threat Assessment

VALIDITY CHECK

stage of the SRM process. Risk managers, therefore, only require the Prevention Vulnerability assessment for each specific event description to complete the likelihood assessment. Security professionals should take care to consider all aspects of the Prevention Vulnerability assessment, using the associated descriptors as a guide, in order to arrive at a reasonable and objective assessment of its measures to hinder specific threats.

Once each event description is assessed on Prevention Vulnerability, the SRM Tool will multiply the Prevention Vulnerability score by the Threat Score for the event (from the Specific Threat Assessment) to generate the Likelihood score for that event. The Likelihood Score will automatically establish a Likelihood Rating from 1 to 5, with accompanying descriptor, as follows:

1. Very Unlikely
2. Unlikely
3. Moderately Likely
4. Likely
5. Very Likely

Impact

The determination of impact in the UNSMS SRM process is the second phase of the Security Risk Assessment. On its surface, judging impact may appear to be relatively simple and it is generally well done within the limited guidance currently available. However, judgment of impact depends on how one attributed values to certain components. For example, if we believe an event will kill a staff member but will have no effect on operations, would we assess the impact of this event as equivalent to an event that has no effect on personnel at all, but completely shuts down an operation? What relative importance does the UN system place on staff, operations and assets? Should the SRM process measure the potential effect of a given event or the actual/historical effect of past examples of the event (incidents)?

Impact is defined as:

A rating of the assessed potential harm that an event would have (if it were to occur) on the Organization. And is also measures on a 1-5 scale from Negligible, Minor, Moderate, Severe and Critical.

It is important to note that the UNSMS SRM model uses the descriptor of “intended effect” when speaking of impact. This is the effect that the security professional judges that the threat actor wishes to achieve if the event were to occur. Security professionals will have to assess the reasonably-expected result of each Event Description (noting that the Event Description often has a reference to the effect in the description itself).

The UNSMS SRM model attributes three components to the measure of Impact for each Event Description:

1. The intended effect on **personnel**
2. The intended effect on **operations** (including assets)

Key Definitions

Impact:

A rating of the assessed potential harm that an event would have (if it were to occur) on the Organization.

Mitigation Vulnerability:

The absence of security countermeasures meant to lower the **Impact** of the event if it were to occur.

Mitigation Vulnerability Assessment:

An assessment of the level to which the UN has implemented effective measures to lower the **Impact** of the event if it were to occur.

Impact = Effect on **Staff** +
Effect on **Operations** +
Mitigation Vulnerability

3. The **Mitigation** Vulnerability

The UNSMS SRM model uses a 1-5 scale, with associated descriptors, to record the measurement of these three components, as follows:

Effect on Personnel

1. No Effect
2. Slightly Injurious Effect
3. Moderately Injurious or Psychologically Traumatic Effect
4. Fatal (individual or small numbers), Severely Injurious or Severely Psychologically Traumatic Effect
5. Catastrophically Fatal Effect (mass casualties)

Effect on Operation

1. No Effect
2. Slightly disruptive effect on programmes and/or slight damage to assets
3. Major disruptive effect on programmes and/or significant damage to assets
4. Short- to medium-term suspension of programmes
5. Long-term suspension or cancellation of programmes

Mitigation Vulnerability Assessment

When discussing Impact, therefore, the following two definitions are required:

- **Mitigation Vulnerability:** inadequate security countermeasures meant to reduce the **Impact** of the event as described, if it were to occur.
- **Mitigation Vulnerability Assessment:** An assessment of the degree to which the UN has implemented effective security countermeasures to lower the **Impact** of the event if it were to occur.

Mitigation Vulnerability refers to the level to which the UN has implemented effective measures to lessen the severity (reducing the level of damage) or the extent (reducing the affected area) of the threat.

Mitigation Vulnerability

1. Mitigation risk management countermeasures and procedures completely in place and consistently effective.
2. Mitigation risk management countermeasures and procedures in place (but may not be consistently effective or may have limitations).
3. Mitigation risk management countermeasures and procedures not completely in place OR not consistently effective.
4. Mitigation risk management countermeasures and procedures not completely in place AND not consistently effective.
5. No mitigation risk management countermeasures and procedures in

place.

Security professionals should take care to consider all aspects in the Mitigation Vulnerability assessment, using the associated descriptors as a guide, in order to arrive at a reasonable and objective assessment of the presence and effectiveness of measures meant to lessen the severity or the extent of the event. The UNSMS SRM Manual cannot provide a comprehensive list of all descriptors and qualifiers for Mitigation Vulnerability and thus risk managers must ensure that they fully consider the multitude of variables in an objective, realistic and evidentiary (i.e. fact-based) manner. As with the General and Specific Threat Assessments, if it is difficult to choose between two descriptors, the SRM Tool allows the user to choose a “half point” between the two (e.g., 2.5 between 2 and 3. In the Risk Analysis steps, this will also include a 0.5 option).

When making the Mitigation Vulnerability assessment, security professionals must record what mitigation measures are in place (and how effective they are) within the e-tool. As with the prevention vulnerability assessment, security professionals reflect only on the measures currently in place and their effectiveness, for example *“First aid kits in all vehicles”* or *“procedures for the use of PPE in place but not consistently implemented”*.

As with the Threat Assessment and Prevention Vulnerability steps above, it is important for the security professional to conduct a “validity check” by comparing the numerical rating made for Impact for one event description with the rating given for other event descriptions to see if there are any anomalies that render the overall assessment inconsistent and/or invalid. Simple questions like, “Does it make sense that the Impact rating for this event is lower than for this other events?” helps ensure consistency throughout assessments.

VALIDITY CHECK

Once the Impact assessment is completed for each Event Description, the SRM Tool will combine the scores for each variable (Effect on personnel, Effect on operations and Mitigation Vulnerability) into a single Impact Rating score for that event. The Impact Score will automatically establish an Impact Rating from 1 to 5, with accompanying descriptor, as follows:

1. Negligible
2. Minor
3. Moderate
4. Severe
5. Critical

Risk Levels

The previous sections illustrated how the Likelihood Ratings and Impact Ratings were determined through a structured, qualitative assessment. This section will focus on Risk Levels and their significance to the SRM process.

The assessment of risk is linked to the assessment of possible future events that may occur and the extent to which those events may harm the organization. The risk posed by a particular threat may therefore be viewed as a factor of the Likelihood of the undesirable event occurring and the

Impact that the event will have if it were to occur (Likelihood x Impact).

The UNSMS SRM model deconstructs Likelihood and Impact into their component parts and establishes a rating for each. The model then reconstructs these ratings into a single Risk Level for each Event Description by multiplying the Likelihood Rating (1-5) by the Impact Rating (1-5). The Risk Level for each Event Description is then attributed a descriptor that identified the level of risk that this event carries for UN operations thus automatically achieving the same result as in the Risk Matrix below:

Risk Score Range	Risk Level
1 to 6	Low
>6 to 10	Medium
>10 to 16	High
>16 to 20	Very High
>20 to 25	Unacceptable

Risk Matrix		Impact				
		Negligible	Minor	Moderate	Severe	Critical
L I K E L Y H O D	Very Likely	Low	Medium	High	Very High	Unacceptable
	Likely	Low	Medium	High	High	Very High
	Moderately Likely	Low	Low	Medium	High	High
	Unlikely	Low	Low	Low	Medium	Medium
	Very Unlikely	Low	Low	Low	Low	Low

Figure 7: Risk Matrix

These Risk Levels are the end result of the Security Risk Assessment and will form the basis for decision-making further on in the SRM process. Risk managers will use this assessment to form risk management strategies and priorities, likely – but not necessarily – first addressing those Event Descriptions that carry the higher risks.

Assigning a Risk Level to an SRM Area or specific mission

As will be seen in Step 8 of the SRM Process, Acceptable Risk balances risk with Programme Criticality. To establish whether an activity can go ahead based on its assigned level of programme criticality, acceptable Risk requires a “level of risk” with which to balance and on which a decision can be made.

As is clear from the process above, an SRM area will have many Event Descriptions associated with it, so what risk level do we assign to an area for the purposes of Acceptable Risk decisions?

For the purposes of making Acceptable Risk decisions, the risk level assigned to an SRM Area, or any other programme or location to which an Ad Hoc SRM Process was applied, shall be the highest risk associated with

any of the events that would be applicable to the programme activity under consideration.

Documenting the SRA

Throughout the SRM Process, the SRM tool provides space to record all manner of information associated with each step. It is very important for the user to ensure accurate and appropriate information is recorded. This record will help support the SRM decision making and provide insight into how changes in the threat and vulnerabilities resulted in new risk judgments when the cycle is repeated.

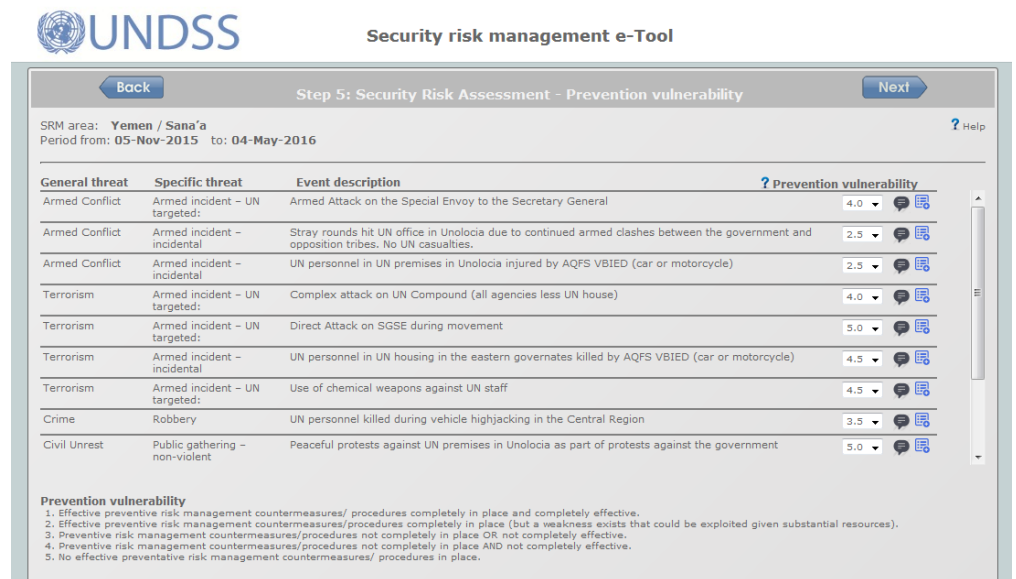


Figure 10: Computer Tool – Prevention Vulnerability Assessment

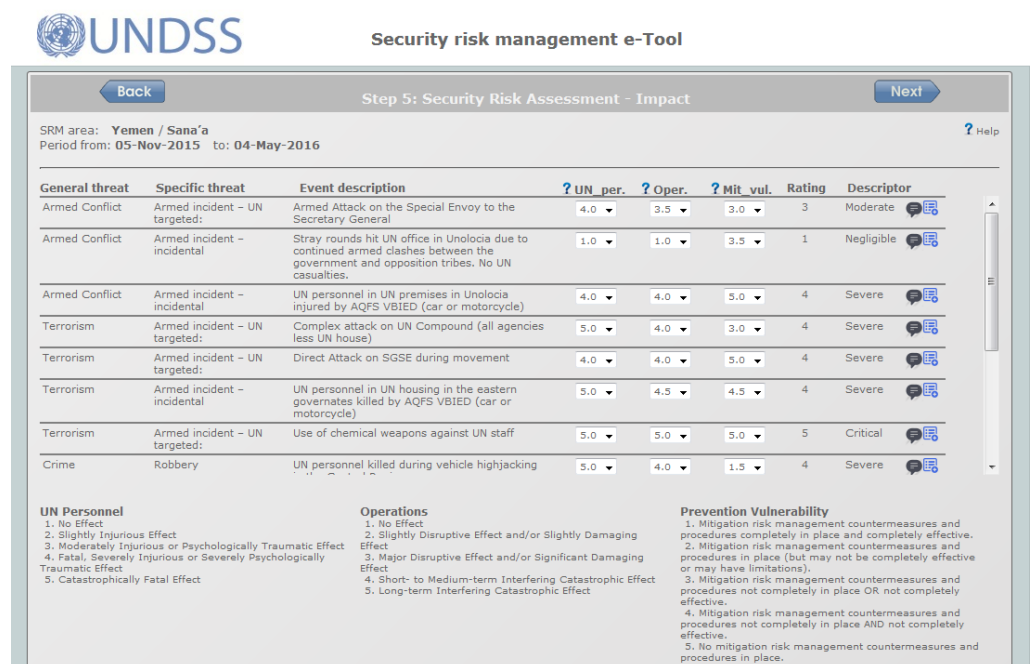


Figure 81: Computer Tool – Impact Assessment



Security risk management e-Tool

Step 5: Security Risk Assessment - Results

SRM area: **Yemen / Sana'a**
 Period from: **05-Nov-2015** to: **04-May-2016**

General threat	Specific threat	Event description	Rating	Descriptor
Armed Conflict	Armed incident - UN targeted:	Armed Attack on the Special Envoy to the Secretary General	3	Medium
Armed Conflict	Armed incident - incidental	Stray rounds hit UN office in Unolocia due to continued armed clashes between the government and opposition tribes. No UN casualties.	2	Low
Armed Conflict	Armed incident - incidental	UN personnel in UN premises in Unolocia injured by AQFS VBIED (car or motorcycle)	3	Medium
Terrorism	Armed incident - UN targeted:	Complex attack on UN Compound (all agencies less UN house)	4	High
Terrorism	Armed incident - UN targeted:	Direct Attack on SGSE during movement	4	High
Terrorism	Armed incident - incidental	UN personnel in UN housing in the eastern governates killed by AQFS VBIED (car or motorcycle)	4	High
Terrorism	Armed incident - UN targeted:	Use of chemical weapons against UN staff	4	High

Figure 12: Computer Tool – Output of the Security Risk Assessment

STEP 6: Security Risk Management Measures

Step 6: Security Risk Management Measures

As noted above, risk management is the process whereby an organization attempts to lower risk by implementing measures to reduce likelihood and/or impact by reducing vulnerabilities.



SRM Measures are identified after specific threats are identified, and only after existing mitigation or prevention measures have been assessed for strengths and weaknesses and when the impact and likelihood of those threats have been evaluated to determine risk. SRM Measures may include information, training, briefings, specialist resources, equipment, physical improvements to premises or facilities, or procedural changes. However, all measures presented must be directly linked to the preceding assessment, assisting to reduce either the likelihood or the impact of an event, or both, and they should be logical, feasible and relevant. Experience, judgement and creativity play a critical role in this step.

Projecting Required SRM Measures

The UN SRM process analyzes threat and vulnerability to assess the risk. If the threat does not change, the only way to lower risk is to lower vulnerability (i.e. increase protection and mitigation). In this way, managing risk means lowering vulnerability by investing in prevention measures and procedures (“prevention vulnerability”) and/or lowering impact by investing in mitigation measures and procedures (“mitigation vulnerability”). Since the SRM Process evaluates each component of risk in a structured way (and records the results of those evaluations in the SRM Tool), it is easy to highlight where the vulnerabilities are and, subsequently, to design SRM measures to address those vulnerabilities.

Remember!

Taking measures to reduce **likelihood** = “**Prevention**”.

Taking measures to reduce **Impact** = “**Mitigation**”.

Present (existing) prevention vulnerability and present (existing) mitigation vulnerability have already been assessed as part of Step 5; and identify where risk management countermeasures/procedures are in place and their effectiveness, on a scale of 1 to 5. This then allows the security professional to determine, based on the existing measures and their effectiveness, what additional measures not currently in place are required, as follows:

- Measures & procedures to reduce likelihood
- Measures & procedures to reduce impact
- Measures & procedures to reduce both likelihood and impact.

If a measure reduces the likelihood or impact of multiple events, it may be necessary to record all the events where risk is reduced.

Selecting SRM measures

Risk management entails making decisions about best options among a number of alternatives in an uncertain environment. Security measures can rarely protect 100% against all threats. The key moment in the execution of any risk management process is therefore when a manager makes the decision to implement a selected course of action. This can include making an affirmative decision to implement new measures, as well as the decision to maintain the current suite of risk management measures (when a risk is already acceptable,

there may be no need to identify and implement additional measures – for more on this, see the section on acceptable risk).

In most cases, the risk management process attempts to strike an economic balance between the impact of risks and the cost of security solutions intended to manage them; measures must be cost-effective. However, as is often the case in the UN, the decision to implement (or not implement) measures may be driven by the importance of a programme, mandate or operation and the measure's ability to save lives, as opposed to its financial cost.

When selecting SRM measures, it will be important to take into account the following:

- **Adverse impacts of SRM measures:** Make sure you have considered any unintended adverse impacts of a particular measure. Your attempts to manage one risk may inadvertently create or increase another risk. For example, measures to manage the risk of an attack on a compound (effective perimeter security, access control, regular guard patrols, etc.) may reduce both the impact and likelihood of an attack, but also distance personnel from local populations (both physically and symbolically), making it harder to conduct operations and implement programmes. Implementing alternative measures, such as engaging in dialogue with the local population, might enhance security whilst minimizing negative appearances.

Other adverse impacts of measures might include increased inconvenience to users (for example, lengthy access controls that delay entry to premises. This could be an irritation to personnel, but even worse it could expose them for longer periods to the threat that was originally to be mitigated), or those that impact the privacy of personnel (for example, the collection of personal information for a security plan). Sometimes these effects are perceived, as opposed to being real, and sometimes it may not be possible to avoid these adverse effects based on the specific risks identified. However, when considering alternative measures we can make efforts to strike a balance between the need to enhance security for the UN and the need to consider the long and short-term adverse impacts associated with each measure.

Remember!

There are four main strategies for managing risk (ACAT):

- Accept
- Control
- Avoid
- Transfer

- **Cost of measures:** As already noted, the costs of potential damage from threats such as terrorism are substantial, but often so are the costs of improved security. However, cost-benefit analysis can be problematic when dealing with security issues, mainly because the benefits are sometimes uncertain and hard to quantify. Determining if a security measure is a sound investment is not always easy. Security is not simply about a financial reward measured against expenditure, but rather the provision of some kind of benefit to others. Knowing that money is being wisely spent on security is key. Some security measures may be implemented at little or no cost, and without the use of complex technology. Updating procedures to improve processes or raising security awareness through communication might incur very little or no cost, while the delivery of training might require a minimal investment. By considering several options before recommending

measures, and if possible, selecting measures that are part of an integrated systems approach (see below), we can more effectively maximize limited financial resources.

- **Additional resources:** For a SRM measure to have success, it is essential that project management methodologies and general management practices support its correct implementation, including where needed communicating with and educating individuals and organizations. Any item of security equipment will also require training, support, maintenance, and multiple other factors to be available if it is to remain operational. For this reason, additional resources – not just the initial cost of a measure - must be considered when selecting SRM measures, in order that they can be implemented effectively and continue to function as anticipated.
- **Time to implement measures:** As already noted, risk management entails making decisions about a number of alternatives; those decisions may differ based on a number of factors, including the relevance of time pressure. Although it may be preferable to take a long-term view to address and manage risks, the realities of an organization's environment dictate that, at times, implementing the risk management process may not be a linear progression. Security professionals, programme managers and decision makers may be required to improvise and truncate steps in the process based on time and resource constraints.¹³ This is not to suggest that short-cuts should be sought, but to ensure that consideration is given as to how long a particular measure may take to implement, and whether the decision to implement will have an influence only in the short-term or over a long period of time. By evaluating the time needed to implement each risk management measure and the resources required, alternative measures might be identified as being more appropriate, meeting time pressures and/or filling gaps where long term measures are not yet fully implemented.

It is not feasible to come up with a comprehensive list of security measures and no single measure will cover all risks. As a security professional, you will be familiar with solutions that work in some locations but not in others. The point is that by following the SRM process, you will be able to tailor your SRM measures specifically to the environment in which you work. The security cell provides an excellent forum for security professionals to develop and consider a variety of options. Options must be feasible, funded, and include resources and timelines that are as comprehensive as possible.

The effects of SRM Measures - reducing Likelihood and Impact

Security measures can have a variety of effects. Risk management measures employed can be considered to *avoid*, *control*, *accept*, or *transfer* risk, and may

¹³ Note that even when the risk management process is expedited or cannot be sequentially executed, it is still appropriate to continue through the cycle after a decision has been made to allow adjustments in execution and to better evaluate performance for the future.

provide benefits in terms of protection, deterrence or acceptance.

Clearly prevention is preferable to mitigation; the desired state is to prevent a threat being presented against the UN. However, the nature of the UN is such that prevention of a threat may often be highly problematic to achieve. We cannot avoid risk altogether. It is therefore important to distinguish between those measures that reduce the likelihood of an event, preventative measures, and those that reduce its impact, mitigation measures

Risk Matrix		Impact				
		Negligible	Minor	Moderate	Severe	Critical
L I K E L Y H O O D	Very Likely	Low	Medium	High	Very High	Unacceptable
	Likely	Low	Medium	High	High	Very High
	Moderately Likely	Low	Low	Medium	High	High
	Unlikely	Low	Low	Low	Medium	Medium
	Very Unlikely	Low	Low	Low	Low	Low

- e.g. Applying shatter resistant film to facility windows, (which have adjoining mullions that can resist the large loads that are collected by the film). This measure will lower impact, by reducing the hazard of flying debris, which could cause injury or death.¹⁴ However, it will not reduce the likelihood of a bomb blast against that premises.
- e.g. Trimming trees and relocating objects near the building that can be used as climbing devices, and ensuring that lamp posts, fences and other building site features are not scalable. This may not reduce the impact of a facility intrusion (there may still be injuries, and/or assets may still be lost), but by preventing access to facility via windows and roofs, the likelihood of an intrusion can be reduced.
- e.g. Delivering security awareness training to develop the competencies, skills, knowledge, values and behavior of personnel to act in a safe and secure manner. This could reduce the likelihood of, for example, the personnel member becoming a victim of a theft, if the training ensures that personnel understand the threats in the environment in which they operate. The training may also help to lower the impact, of, for example, a carjacking, if the training includes guidance on what to do in that type of event.

Integrated Systems Approach

Although measures that reduce the likelihood of an event and those that mitigate its impact are assessed one by one, multiple measures are implemented to simultaneously reduce impact and likelihood. The combined effects of several security measures is a systems approach, integrating physical, procedural,

¹⁴ In the event of a blast threat, the effectiveness of mitigation measures (particularly in the case of retrofit upgrades as opposed to new-builds) depends to a great extent on the structural details of the building.

technical and human aspects of security. In the case of UN premises, the systems approach is based on the effective use of the following principles:

- **Deter** – physical and procedural security that attempt to prevent undesirable action against the premises by influencing the attacker’s decision making. Deterrence is a psychological measure; it increases the perception of effort or fear of failure in the mind of the attacker.
- **Detect** – measures to detect and assess planning, (or actual attempts) by threat actors to penetrate the security perimeter or to test the effectiveness of the security system in place.
- **Delay** – physical, technical, procedural or psychological barriers to restrict movement and to allow time for appropriate response (by security or host Government forces).
- **Deny** – the ability to oppose or negate the effects of an action against the premises, including denying access to information on the layout and contents of the premises. The premises security system must be designed to deny identified threat actors the ability to carry out a successful harmful action against the premises.

The integration of the principles outlined in the Four Ds above requires the concept of Concentric Layers of Security (Defence in Depth). Proper premises security requires a system designed with sufficient diversity and redundancy so that the strength of one particular component offsets the weakness of another. Components of the security system must be designed in sufficient number of layers to make it more difficult to defeat the whole system. All United Nations premises require at least two physical layers of security between personnel or valuable assets and the areas beyond direct United Nations control, including a system to only allow authorized persons, vehicles and other items to cross these layers (access control). The principle of concentric layers of security also requires UNSMS officials responsible for the premises to coordinate with areas of responsibility of the host government outside of the premises.

Decision-making and Implementation

Risk is reduced only after the management measures have been implemented. Once you have selected your appropriate SRM measures based on how they reduce likelihood and impact, and having considered whether they are fundable and practical given your timelines, decision-makers need to consider the feasibility of implementing options. When providing decision-makers with your recommendations, you need to be able to present your options, and their strengths and weaknesses, clearly and understandably in order to ensure that decisions are informed by a common understanding of the organization’s risks. Information should be tailored to the needs of leadership. Decision makers should have a clear understanding of the present risk; the security risk based on the threats; the security measures and procedures currently in place; the projected risk; and, the expected security risk if recommended security measures and procedures were to be in place. Once a decision is made, there must be a strong commitment for implementing the mitigation plan.

Once SRM measures are identified they are approved by the DO/SMT¹⁵. USG DSS authorization is required for Evacuation and/or Relocation of UNSMS personnel, continuation of activities associated with very high residual risk, lifting of Evacuation and/or Relocation status or in support of a recommendation for danger pay. When the SRM process recommends these measures and they are approved by the DO with the SMT they must be authorized by USG DSS unless lives are threatened and communications are lost¹⁶.

Once security risk management measures and processes are approved at the appropriate level they are requirements. As part of this approval process, an Implementation Plan (part of the e-tool) must be developed in order to ensure that these measures are put in place and by ongoing monitoring and review, to ensure that they are completed in a timely and effective manner. As already noted, all SRM measures must be logical, practical, realistic, cost effective and capable of being implemented within the context of the SRM area.

If a new operation or programme is established then a new time scale for implementation of the security risk management measures and procedures needs to be established to include clear indications of the risk level that these programmes face before and after full implementation of SRM measures.

Given that the SRM process relates very clearly to a defined SRM area, the SRM process allows sufficient flexibility to ensure that the measures relate specifically to that area, avoiding the need for minimum measures for the whole country. However, certain mandatory requirements for all duty stations also need to be implemented. For example, the requirement for all staff to have completed BSITF II, for PEP kits to be on hand, and for security plans to be updated and made available, are SRM measures that are integral to the Framework of Accountability. Although these may not be captured in the Implementation Plan for the SRM area, they are requirements and a progress update should therefore be provided to determine whether implementation for each measure is completed or not.

Monitoring risk clearly overlaps with the implementation process, whereby monitoring helps to continuously manage risks – see the next chapter for more on this.

¹⁵ Although the area SRM is completed for a specific area where there may be an ASC in place. Authority for approval of all SRM processes remains with the DO in accordance with the Framework for Accountability.

¹⁶ UNSMS SPM

UNDSS Security risk management e-Tool

SRM area: **Yemen / Sana'a**
 Period from: **05-Nov-2015** to: **04-May-2016**

General threat	Event description	Present Risk	Present Prevent. Vulnera.	Prevention	Present Mitigat. Vulnera.	Mitigation	Prevention & Mitigation
Armed Conflict	Armed Attack on the Special Envoy to the Secretary General	Medium	4.0	0	3.0	0	0
Armed Conflict	Stray rounds hit UN office in Unolucia due to continued armed clashes between the government and opposition tribes. No UN casualties.	Low	2.5	0	3.5	0	0
Armed Conflict	UN personnel in UN premises in Unolucia injured by AQFS VBIED (car or motorcycle)	Medium	2.5	0	5.0	0	0
Terrorism	Complex attack on UN Compound (all agencies less UN house)	High	4.0	0	3.0	0	0
Terrorism	Direct Attack on SGSE during movement	High	5.0	0	5.0	0	0
Terrorism	UN personnel in UN housing in the eastern governates killed by AQFS VBIED (car or motorcycle)	High	4.5	0	4.5	0	0
Terrorism	Use of chemical weapons against UN staff	High	4.5	0	5.0	0	0
Crime	UN personnel killed during vehicle highjacking in the Central Region	High	3.5	0	1.5	0	0
Civil Unrest	Peaceful protests against UN premises in Unolucia as part of protests against the government	Unacceptable	5.0	0	5.0	0	0
Civil Unrest	UN offices attacked after declaring election results 1	Low	3.0	0	4.0	0	0

Prevention Vulnerability
 1. Preventive risk management countermeasures/procedures completely in place and completely effective.
 2. Effective preventive risk management countermeasures/procedures completely in place (but a weakness exists that could be exploited given substantial resources).
 3. Preventive risk management countermeasures/procedures not completely in place or not completely effective.
 4. Preventive risk management countermeasures/procedures not completely in place and not completely effective.
 5. No preventative risk management countermeasures/procedures in place.

Mitigation Vulnerability
 1. Mitigation risk management countermeasures and procedures completely in place and completely effective.
 2. Mitigation risk management countermeasures and procedures in place (but may not be completely effective or may have limitations).
 3. Mitigation risk management countermeasures and procedures not completely in place or not completely effective.
 4. Mitigation risk management countermeasures and procedures not completely in place and not completely effective.
 5. No mitigation risk management countermeasures and procedures in place.

Figure 13: Computer Tool – Add Recommended Security Risk Management Measures

UNDSS Security risk management e-Tool

SRM area: **Yemen / Sana'a**
 Period from: **05-Nov-2015** to: **04-May-2016**

General threat	Event description	Present Prevention Vulnerability	Present Mitigation Vulnerability	Present risk	Projected Prevention Vulnerability	Projected Mitigation Vulnerability
Armed Conflict	Armed Attack on the Special Envoy to the Secretary General	4.0	3.0	Medium	2.0	2.0
Armed Conflict	Stray rounds hit UN office in Unolucia due to continued armed clashes between the government and opposition tribes. No UN casualties.	2.5	3.5	Low	2.0	2.0
Armed Conflict	UN personnel in UN premises in Unolucia injured by AQFS VBIED (car or motorcycle)	2.5	5.0	Medium	2.0	3.0
Terrorism	Complex attack on UN Compound (all agencies less UN house)	4.0	3.0	High	2.5	2.0
Terrorism	Direct Attack on SGSE during movement	5.0	5.0	High	2.0	2.0
Terrorism	UN personnel in UN housing in the eastern governates killed by AQFS VBIED (car or motorcycle)	4.5	4.5	High	3.0	2.5
Terrorism	Use of chemical weapons against UN staff	4.5	5.0	High	2.5	3.0
Crime	UN personnel killed during vehicle highjacking in the Central Region	3.5	1.5	High	2.0	1.5
Civil Unrest	Peaceful protests against UN premises in Unolucia as part of protests against the government	5.0	5.0	Unacceptable	3.0	2.0
Civil Unrest	UN offices attacked after declaring election results 1	3.0	4.0	Low	3.0	3.0

Prevention Vulnerability
 1. Preventive risk management countermeasures/procedures completely in place and completely effective.
 2. Effective preventive risk management countermeasures/procedures completely in place (but a weakness exists that could be exploited given substantial resources).
 3. Preventive risk management countermeasures/procedures not completely in place or not completely effective.
 4. Preventive risk management countermeasures/procedures not completely in place and not completely effective.
 5. No preventative risk management countermeasures/procedures in place.

Mitigation Vulnerability
 1. Mitigation risk management countermeasures and procedures completely in place and completely effective.
 2. Mitigation risk management countermeasures and procedures in place (but may not be completely effective or may have limitations).
 3. Mitigation risk management countermeasures and procedures not completely in place or not completely effective.
 4. Mitigation risk management countermeasures and procedures not completely in place and not completely effective.
 5. No mitigation risk management countermeasures and procedures in place.

Figure 14: Computer Tool – Projected Vulnerability



Security risk management e-Tool

		Present and projected risk		Submit to DO	
SRM area: Yemen / Sana'a Period from: 05-Nov-2015 to: 04-May-2016					
General threat	Event description	D/I	Present risk	Projected risk	
Armed Conflict	Armed Attack on the Special Envoy to the Secretary General	Direct	Medium	Low	
Armed Conflict	Stray rounds hit UN office in Unolocia due to continued armed clashes between the government and opposition tribes. No UN casualties.	Indirect	Low	Low	
Armed Conflict	UN personnel in UN premises in Unolocia injured by AQFS VBIED (car or motorcycle)	Indirect	Medium	Low	
Terrorism	Complex attack on UN Compound (all agencies less UN house)	Direct	High	Medium	
Terrorism	Direct Attack on SGSE during movement	Direct	High	Low	
Terrorism	UN personnel in UN housing in the eastern governates killed by AQFS VBIED (car or motorcycle)	Indirect	High	Medium	
Terrorism	Use of chemical weapons against UN staff	Direct	High	Medium	
Crime	UN personnel killed during vehicle highjacking in the Central Region	Direct	High	Medium	
Civil Unrest	Peaceful protests against UN premises in Unolocia as part of protests against the government	Direct	Unacceptable	High	
Civil Unrest	UN offices attacked after declaring election results 1	Direct	Low	Low	
Civil Unrest	UN Offices damaged by violent protests caused by dissatisfaction of weakening/dismantled peace agreement	Direct	High	High	
Civil Unrest	UN personnel injured during violent protests caused by dissatisfaction of weakening/ dismantled peace agreement	Direct	Medium	Low	

Figure 15: Computer Tool – Projected Risk and Submission of SRM to the DO

Step 7: Security Risk Management Implementation



STEP 7: SRM Implementation

Risk is reduced only after the management measures have been implemented. Once the appropriate SRM measure(s) are selected based on how they reduce likelihood and/or impact, and having considered whether or not they are funded, resourced and practical given the timelines, decision-makers need to consider the feasibility of implementing options. When providing decision-makers with recommendations, security professionals need to be able to clearly present available options, and their strengths and weaknesses, in order to ensure that decisions are informed by a common understanding of the organizations' risks. Information should be tailored to the needs of leadership and be presented as part of an Implementation Plan.

Once a decision is reached, there must be a strong commitment for implementing the mitigation/prevention plan. Without this stage operating effectively, the entire security risk management process could fail. Leadership should therefore encourage security actors and appropriate third parties (such as engineering specialists, telecommunications experts, security providers, etc.,) to adopt comprehensive project management approaches that will document the planning, organising, and managing of resources necessary for the successful implementation of the risk management process, taking into account the following aspects of the Implementation Plan.

- **Prevention/mitigation measure:** detail the specific measure proposed.
- **Prevention/mitigation objective:** How does the measure actually manage the risk? Does it reduce either likelihood or impact, or both?
- **Resources/Costs:** What resources are required? Consider, for example, additional funding or collaboration. Consider whether this is a one-time cost or whether there are recurring costs (e.g. for maintenance, training, etc.).
- **Actor responsible for implementation:** Determine the appropriate manager responsible for identifying and implementing the risk security risk management plan. He or she must have the knowledge and/or resources to implement the plan. Risk management measures or procedures will not be effective without an engaged risk manager who has the authority, granted to him/her by senior leadership, to carry out implementation. Irrespective of who is tasked to implement the measures, the SMT has responsibility to ensure that implementation is completed.
- **Timeframe for implementation:** Determine the time needed to complete each action and when the expected completion date should be. Be realistic with implementation timeframes, taking into account how long actions might require, and bearing in mind that resources and/or funding may take time to become available, particularly for measures related to infrastructure or specialized equipment such as armored vehicles, as opposed to those, such as SOPs, that can be implemented quickly and with minimum or no cost. In the event of long lead times for implementation, alternative and/or temporary measures should be considered to ensure that there are no gaps in the SRM process and the level of remaining risk in the interim period is

still considered to be acceptable.

- **Progress update:** State whether implementation has not yet started, is in progress or completed. Identify actions and steps needed to implement the mitigation/prevention strategy. What specific actions are needed? Include only those stakeholders relevant to the step, action, or decisions and make sure progress is clearly documented. Appropriate decisions, agreements, and actions resulting from a meeting would be required for progress, not merely the fact that the meeting was held. Look for evaluation, proof, and validation of criteria met. Consider, for example, metrics or test events.

Budgeting and funding

Funding for mitigation or prevention measures may come from a number of different sources:

Note that all of these measures apply to the specific SRM area identified at the outset of the SRM process

Jointly Financed Activity (JFA):

Given the dual responsibility of UNDSS to provide for the safety and security of staff, delegates and visitors at the main locations of the United Nations as well as the safety and security of the United Nations system operations in the field, the Department's activities are financed both from the regular budget and on a cost-sharing basis and reflected as part of Jointly Funded Activity(ies).

The cost share budget is structured to reflect three primary components of UNDSS: the Division of Regional Operations, the Field Support Service and Field Security Operations. Understanding that the JFA is based on the principle of collective responsibility for security and established cost sharing arrangements, UNDSS field-related costs, which are incurred either in the field or at headquarters locations through the provision of operational support, are shared on a proportional basis between UNSMS organisations.

For the most part, the JFA provides the over-arching framework for the security team on the ground and allows for the provision of UNDSS personnel and their associated costs (staffing, travel within their SRM area, rental of premises, vehicles, communications equipment, etc.). Any decision to augment this structure in any way must be justified and requires the approval and funding of the Designated Official and agreement of the Security Management Team (SMT) and would be included as part of the Local Cost Share Budget (see below).

Local Cost Share Budgets:

The Local Cost Share Budgets (LCSB) are decided by the Designated Official in conjunction with the SMT / UN Country Team (UNCT) and should only reflect common services that are provided for the risk management of all staff. They are dependent on the approved security risk management measures and particular circumstances on the ground. As agreed by the IASMN, LCSB activities are based on the eight major categories below:

- **Identification Programme.** Amount approved for common badge

Include all the Costs –
When selecting security risk management measures all costs need to be identified e.g.s.

An Armoured Vehicles may cost \$135,000 but there are associated costs of AV driver training, increased servicing charges, increased fuel costs.

A radio operator may be paid \$22,000 a year but there are associated costs for staff training, family entitlements, insurance, travel etc. that are substantially higher than the basic wage.

system implemented at duty station with description of the activity and details of funding required.

- **Operational support.** The number, function and level of approved additional national security personnel above the UNDSSDSS authorized staffing providing a detailed description of each position and the details of the funding required.
- **Security Training.** Amount approved for conducting security related training for UN personnel, such as SSAFE, warden training etc., providing description of the activity and details of funding required.
- **Communications Structure.** Amount approved for common communications structure requirements providing description of the activity and details of funding required.
- **Crisis Management Centre.** Amount approved for operating a common Crisis Management Centre providing description of the activity and details of funding required.
- **Guard Force.** Amount approved for operating, contracting or other requirements for a guard force at UN House or other common guard or reaction force arrangements at the duty station providing description of the activity and details of funding required.
- **Psychosocial Support.** Amount approved for obtaining the services of a stress counsellor as required for the duty station providing description of the activity and details of funding required.
- **Vehicle Requirements.** Amount approved for special vehicle requirements such as armored vehicles or vans for common usage providing description of the activity and details of funding required.

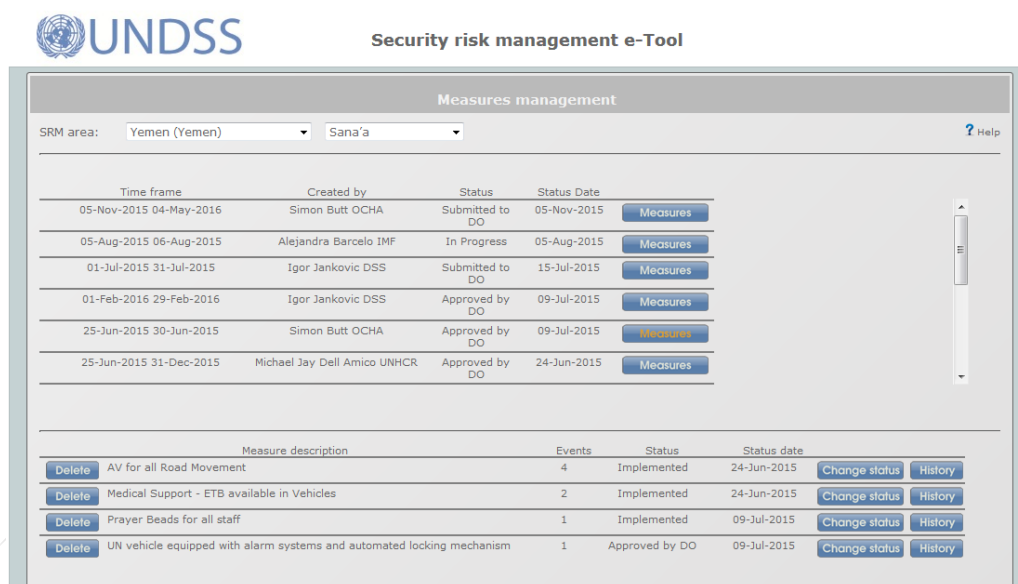
The approval process is to be completed at the country level by end August. Regardless of the costs, all field offices are to prepare and input the budget information on UNSMIN for the following fiscal year (SMT approval is not required at this point):

- In the event that the LCSB does not exceed \$150,000, the approval process remains in country. In such cases, the DO/SMT will have until the end of December that year to approve the process at which time the information regarding the status of the LCSB can be adjusted to reflect “approved”.
- In the event that the LCSB exceeds \$150,000:
 - By the end of Oct, the LCSB must be presented and approved by the DO/SMT.
 - Once approved by the DO/SMT, this information is to be uploaded into the UNSMIN site along with any supporting documents, at that point:

- The CSA/ SA will request a review by DRO and the UNDSS/EO. DRO will review the substantive elements while the EO will review the financial aspects.
- Simultaneously, the SFPs of the UNSMS organizations will review and submit comments, if any.
- During their review, both DSS and the SFPs of the UNSMS organizations may request additional information/justification and request a revision of the budget as necessary. LCSBs are endorsed only if all the issues raised during the review process have been fully addressed, including revision of the LCSB as necessary. This process is to be completed by mid-December of each year.
- At this point (mid-December) UNDSS will endorse all budgets.

Organization-specific budgets:

Certain SRM measures which are not common for all agencies, funds and programmes may be funded by individual organisations. Examples may include security guards at an agency-specific facility or compound. Agencies may have their own budgets or sources of funding for these measures.



Measures management

SRM area: Yemen (Yemen) Sana'a Help

Time frame	Created by	Status	Status Date
05-Nov-2015 04-May-2016	Simon Butt OCHA	Submitted to DO	05-Nov-2015
05-Aug-2015 06-Aug-2015	Alejandra Barcelo IMF	In Progress	05-Aug-2015
01-Jul-2015 31-Jul-2015	Igor Jankovic DSS	Submitted to DO	15-Jul-2015
01-Feb-2016 29-Feb-2016	Igor Jankovic DSS	Approved by DO	09-Jul-2015
25-Jun-2015 30-Jun-2015	Simon Butt OCHA	Approved by DO	09-Jul-2015
25-Jun-2015 31-Dec-2015	Michael Jay Dell Amico UNHCR	Approved by DO	24-Jun-2015

Measure description	Events	Status	Status date
AV for all Road Movement	4	Implemented	24-Jun-2015
Medical Support - ETB available in Vehicles	2	Implemented	24-Jun-2015
Prayer Beads for all staff	1	Implemented	09-Jul-2015
UN vehicle equipped with alarm systems and automated locking mechanism	1	Approved by DO	09-Jul-2015

Figure 16: Computer Tool – Measure Management

Step 8: Acceptable Risk



STEP 8: Acceptable Risk

Risk management has three important principles that relate to how the United Nations Security Management System (UNSMS) deals with questions of acceptable risk:

- **Do not accept unnecessary risk.** There is no benefit in accepting unnecessary risk if it does not help the UN achieve its objectives.
- **Accept risk when benefits outweigh risks.** We cannot eliminate all risks – that would be too rigid and costly. On the other hand, avoiding all risks does not help the UN achieve its objectives.
- **Make risk management decisions at the right level.** This means that the organization must ensure that decisions on risks are taken at the level of delegated authority. UN personnel and managers must not assume risk for which authority has not been received.
- **Everything reasonable should be done to reduce the risk.** We must always try to lower risk whenever feasible

Acceptable Risk Model

Based on these principles, the UNSMS “Acceptable Risk Model” balances the security risk with programme benefits (called “Programme Criticality”). There are four levels of Programme Criticality in line with the levels of risk produced in the Step 5 - Security Risk Assessment (SRA).

The Acceptable Risk Model also distinguishes between activities carried out by UN personnel and activities carried out by implementing partners as part of a UN programme. The Acceptable Risk Model only deals with activities conducted by UN personnel. Personnel of implementing partner organizations conducting activities as part of a UN programme are not covered by the UNSMS so these activities are not considered in the Acceptable Risk Model.

Figure 14 below shows the schematic of the Acceptable Risk Model. Security Risk Management, encompassed in the tool explained in all the proceeding chapters of this Manual, is used to establish the present level of risk associated with a particular area or activity. A separate tool, called the Programme Criticality Tool (explained in Annex C), is used to establish which of four levels of Programme Criticality any activity involving UN personnel falls. The Acceptable Risk Model then establishes the maximum level of security risk that is acceptable for each level of Programme Criticality.

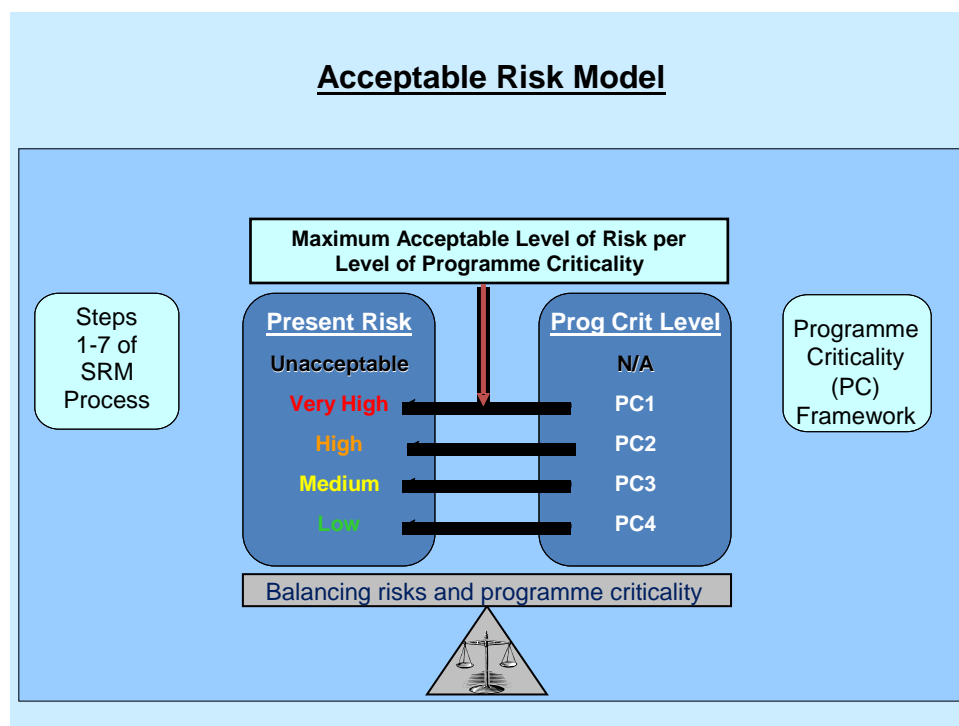


Figure 17

There is a level of risk that is unacceptable no matter what activity UN personnel may wish to conduct. This level of unacceptable risk is when an event is assessed to have the highest level of likelihood (Very Likely) and the highest level of impact (Critical Impact). The only security risk management option in this situation is to avoid the risk, i.e., move people away from the location or situation until the required security measures are in place and functioning to bring the risk down to acceptable levels (until the risk is at least Very High).

Acceptable Risk Balanced with Programme Criticality

Whether risk of an activity is acceptable at any level lower than “unacceptable” is determined by the level of Programme Criticality of the activity (as per Figure 2 above). The Programme Criticality Tool (Annex C) is used to establish the levels of Programme Criticality for this purpose.

We must always try to lower risk whenever feasible

If a UNSMS organization has done all it can to lower the security risk, and the security risk is assessed as Very High, then that organization would be able to conduct only PC1 activities, and only if:

- The Executive Head of that organization approves that the activity is a PC1 activity; and
- The Under-Secretary-General for Safety and Security gives the final clearance.

If a UNSMS organization has done all it can to lower the security risk, and the security risk is assessed as High, then that organization would be able to conduct PC1 and PC2 activities but only if:

- Representative of the organization of the UN system at the country

level approves that the activity is either a PC1 or PC2 level activity; and

- The Designated Official gives the final clearance.

If a UNSMS organization has done all it can to lower the security risk, and the security risk is assessed as Medium, then that organization would be able to conduct PC1, PC2 and PC3 activities only if:

- Representative of the organization of the UN system at the country level approves that the activity is either a PC1, PC2 or PC3 level activity; and
- The Designated Official gives the final clearance.

Finally, if a UNSMS organization has done all it can to lower the security risk, and the security risk is assessed as “Low” by the SRA, then that organization can conduct any activity (PC1, PC2, PC3 and PC4).

The above explanation shows that the more we invest in security risk management measures the more activities we can conduct because the investment in SRM measures has lowered risk.

As noted in Step 5 above, for the purposes of making Acceptable Risk decisions, the risk level assigned to an SRM Area, or any other programme or location to which an *ad hoc* SRM Process was applied, shall be the highest risk associated with any of the events that would be applicable to the programme activity under consideration.

Programme Criticality Tool

How an activity is assigned a certain level of Programme Criticality is covered by the use of the Programme Criticality Tool. Details on how that tool works are found in Annex C below.

As noted above, the output of the Programme Criticality Tool (an assigned “PC Level” for each activity) becomes the input for a decision on Acceptable Risk.

Step 9: Review



STEP 9: Review

Why Carry out Monitoring and Evaluation?

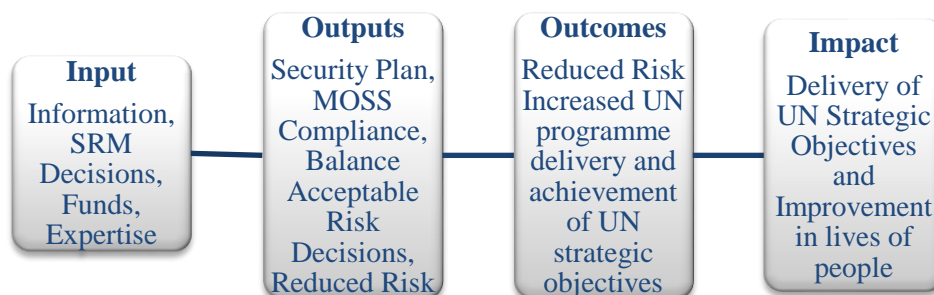
The simple answer is that only through monitoring and evaluation can we ensure that the risk has been reduced and the United Nations programmes are able to deliver within acceptable levels of risk. Only with effective monitoring of implementation and evaluation of the end results do we know whether the risk management decisions have been genuinely effective and achieved the desired, predicted results.

Review enhances the effectiveness of the SRM process by establishing a link between the past, present and future. It extracts knowledge of the past and ongoing security risk management information to fine tune, re-orientate and plan.

Purpose. The purpose of monitoring and evaluation is to improve the effectiveness of the security risk management measures and increasingly enable programme delivery at an acceptable level of risk.

- **Monitoring.** Monitoring aims primarily to provide security advisers and the SMT early indications of progress, or lack thereof, in implementation of the security risk management measures. It is an objective process of checking activities. Monitoring is what was previously generally referred to as “compliance”.
- **Evaluation.** Evaluation is assessing the progress and effectiveness in achieving the desired SRM aim. It is ensuring that the implemented activities are leading to the desired and expected outcomes. Between monitoring and review, review is the most important if we are to ensure that SRM is fit for purpose.

Within the SRM process there are inputs, outputs, outcomes and impacts. The SRM aim is focused on the outcome – enabling United Nations programme delivery at an acceptable level of risk – but only has full control of the inputs and outputs:



You Monitor the implementation of the Outputs

You Evaluate the Outcomes

Security Risk Management Areas Monitoring and Review

Monitoring Tools. The UN SMS already has several effective formal tools and forums for monitoring the implementation of agreed SRM decisions:

- **SMT** – The security briefings to the SMT allow the routine monitoring of the implementation of the agreed SRM measures. It is within this forum that implementation is monitored in line with the accountabilities and responsibilities of the SMT.
- **Security Cell** – The security cell is the center for the application of security expertise in a country to ensure that not only the correct advice is given to the SMT but that those decisions are implemented.
- **UNDSS DRO regional desks and the Peacekeeping Operations Support Section (POSS)** – The regional desks and POSS constantly monitor the SRM process in the countries and missions assigned to them, and where necessary recommend remedial action. Where necessary, their observations can be elevated to DRO level, and ultimately to the USG UNDSS as required.
- **Alternative monitoring** – Depending on the situation and needs in the designated area, a security adviser, in consultation with the SMT, may implement alternative monitoring. These may include:
 - **Spot Checks** on personnel, residences, offices, vehicles, missions, guard posts, and any other security measure. These spot checks can reveal where security risk management measures have, or have not, been implemented and can indicate which areas require additional focus;
 - **Surveys.** Surveys of personnel, agencies or programme managers often reveal details of implementation or non-implementation of security risk management measures or gaps in knowledge of policies and procedures that are not apparent in other forms of monitoring.
 - **External monitoring.** External checks on implementation either internally in the country e.g. agency FSA, or the security cell carry out check and provide supportive feedback for agencies other than their own. Alternatively neighboring SRM Areas can check each other.

Apart from the compulsory monitoring through the SMT and Mandatory Self-Assessment, it is the decision of the DO/ASC in consultation with the SMT/ASMT as advised by the SA in consultation with the Security Cell on what type of monitoring best ensures that security risk management measures are being implemented in a timely and effective manner.

Evaluation Tools. The principal driver for the evaluation of the effectiveness of the security risk management in the Designated Area is the regular, periodic review of the SRM outcomes. However, restarting the SRM process is not necessarily an active evaluation of effectiveness. Alternatives for evaluation of effectiveness include:

- **Assessment of Indicators.** Since the aim is to enable acceptably safe programme delivery, the assessment of security and programme delivery indicators can be extremely revealing. *For example a comparison of incidents affecting the UN before and after the implementation of the new security risk management measures is a crude indicator of reduction of risk. A simple comparison of the number of programme missions completed or personnel deployed to the field before and after the new security risk management measures can indicate whether UN programme delivery is being better enabled.*

Top Tip:

When considering an exercise you need to be clear whether it is a training exercise or a testing exercise. **Training exercises should lead the trainees through the process to success. Testing exercises should provide the scenario and allow staff to act according to their role.**

Analysis can be as simple or complex as desired, but it is important to ensure that all factors have been considered. Any system is interconnected and the context of a single indicator often changes over a period of comparison. *For example it may be found that despite the implementation of new security risk management measures, incidents affecting the UN have gone up by 10%. However, if more effective decisions on acceptably safe programme delivery have been taken, there may be an increase of 80% in the number of missions and personnel deployed. In this case the increase of 10% in incidents while there has been an 80% increase in missions in fact shows that the security risk management measures have been very effective, while enabling increased programme delivery.*

- **Client Surveys.** Surveys of agencies, funds, programmes and missions, often reveal details on effectiveness of security risk management measures or gaps in policies and procedures that are not apparent in other forms of monitoring.
- **Exercises.** Exercises are useful tools for training and validating security risk management measures. Security personnel should conduct exercises to train and also to test plans and capabilities while promoting various roles and responsibilities during a crisis. Successfully conducting an exercises involves considerable coordination among All key stakeholders and managers. There are some key stages essential to conducting successful exercises:
 - a. **Establish a foundation:** Create a base of support from the appropriate entities and senior managers, develop a timeline for training and exercising including milestones, identify an exercise planning team, schedule planning meetings. Training and exercises cost resources so you need support from management and you need to demonstrate utility.
 - b. **Design and development:** Building on the exercise foundation, establish SMART objectives (what are you exercising?), scenario design, documentation, logistics and develop an evaluation (how will you measure success or failure?) and improvement methodology.
 - c. **Conduct the exercise:** This includes the set-up, briefings, facilitation, control, evaluation and wrap up activities.
 - d. **Evaluation:** This includes a formal evaluation of the exercise,

Remember!

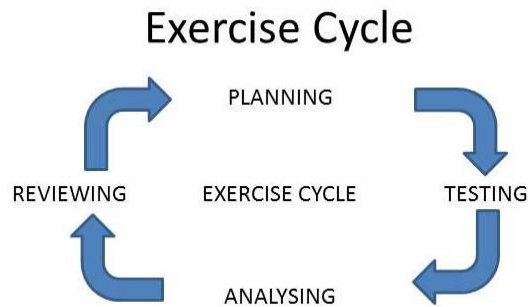
An exercise where everything runs perfectly is unrealistic and provides no information that will lead to improvements.

Test exercises should be challenging at an appropriate level for the players.

an integrated analysis, after action report and improvement plan. Recommendations and need to be implemented and tracked throughout the process.

- e. **Improvement Planning:** corrective actions identified in the evaluation phase are assigned with due dates to responsible parties, tracked to implementation and validated in following exercises.

Exercise Cycle - the following diagram illustrates the cyclical nature of process improvement using training and exercising.



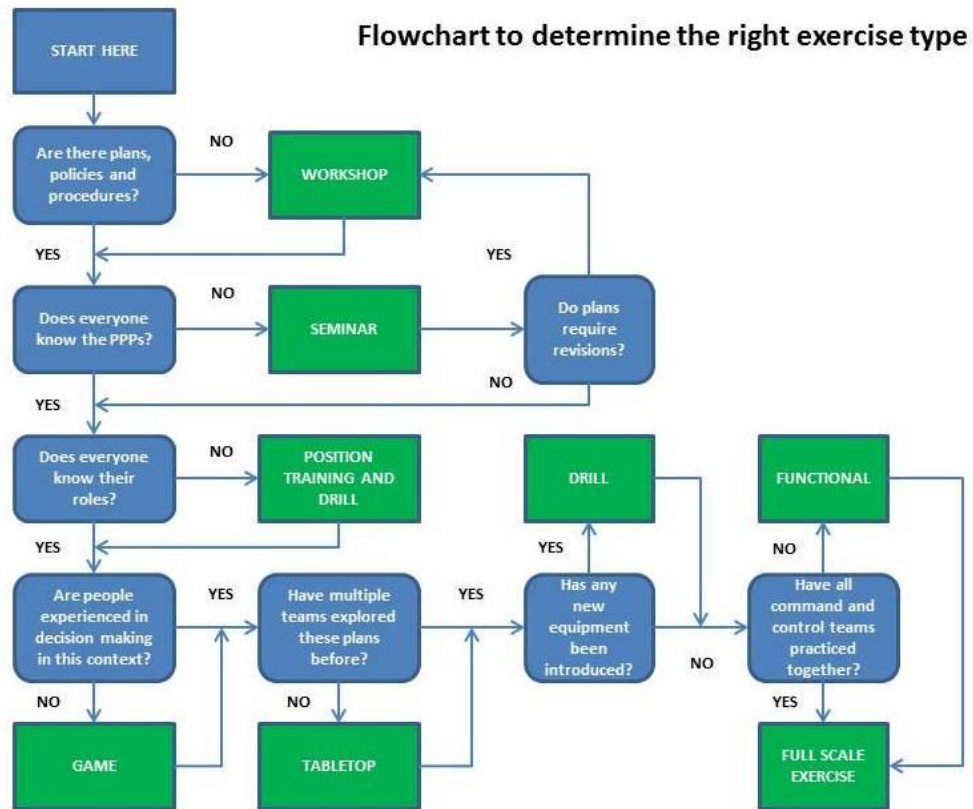
Exercise Types. Exercises can be broadly categorized as discussion based or operation based, and are appropriate at different levels of your planning. Avoid the temptation to jump into operation based exercises too early; people need to learn their roles and gain confidence and knowledge.

- **Discussion based exercises** familiarize participants with current plans and procedures, policies, agreements, or may be used to develop new procedures. Discussion based exercises include:
 - Seminars use different strategies such as lectures, panel discussions, case studies etc. They are informal discussions based on policies, procedures, protocols, concepts, resources and ideas.
 - Workshops are more participative and are effective for team building, problem solving, information sharing and brain storming.
 - Tabletop exercises (TTXs) consist of informal facilitated discussions of simulated emergencies among key personnel. The purpose of a TTX is to test existing plans without incurring costs associated with deploying resources. Most issues involving security risk measures can be resolved using TTXs.
 - Games such as red team exercises (Red Teaming) are a fairly advanced form of testing assessments, plans and procedures. Red team exercising is normally associated with assessing vulnerabilities and limitations of systems or structures and is well designed for testing the effectiveness and vulnerability reduction of security

risk management measures. An independent group challenges an organization to improve its effectiveness by actively looking for vulnerabilities in a system and suggesting methods of exploiting the vulnerabilities. Key in red team exercises is the application of realistic capabilities, intents and limiting factors of the threat e.g. by the independent group. There is no point in a Red Team exploiting vulnerabilities to IEDs when no threat actors in the designated area have demonstrated any intent or capability of using IEDs. An unlimited Red Team will always win.

- **Operations-based exercises** validate plans, policies, agreements and procedures; clarify roles and responsibilities and identify resource gaps in an operational environment. Operational-based exercises include:
 - Drills are coordinated activities that test a specific operation or function. Drills are for skills development and maintenance on new equipment or procedures.
 - Functional exercises (FEs) or command post exercises examines and validates coordination mechanisms, communication and command and control between different operational entities. Fes are highly stressful and involve notional deployment of personnel and resources in real time. FEs are great for testing coordination between CMTs, SMTs, ICPs and UNHQ.
 - Full Scale Exercises (FSEs) replicate a real world response with actual deployment of resources. FSEs are resource costly but essential in the later stages of your testing plan.

So what exercise and when? The following diagram illustrates points in your planning process when the different types of exercises are most appropriate.



Remember you want to build capacity and confidence, so increase complexity as capacity grows.



External Evaluations.

Output. The output of monitoring provides oversight of the implementation of agreed security risk management measures. The output of review and evaluation informs the effectiveness of security risk management measures and therefore informs the vulnerability assessments.

Support: DSS Guidance on SRM Process Management, Support and Oversight

DSS Guidance on SRM Process Management, Support and Oversight

SRM Flow Process

Prior to commencing the SRM process, the Senior Security Professional should consult with all Security Professionals and SRM actors to identify important and priority components for each step [in plain language, the Senior Security Professional should have a discussion about the SRM process before putting pen to paper – or fingers to keyboard – and this means a security cell meeting]

Designation of the “SRM Area”. The Designated Official, in consultation with the Security Management Team, designates SRM Area(s).

SRM Areas Process. Senior Security Professional with responsibilities for a SRM Area¹⁷ initiates the SRM process for this area using the SRM e-tool through the following;

Creating a specific SRM; (area? Revision? Process?);

Designating SRM actors for the specific SRM, including the following:

SRM actors with delegated authority by the Senior Security Professional to contribute to or develop specific SRM steps¹⁸;

SRM actors who are invited by the Senior Security Professional to comment on specific SRM steps¹⁹;

SRM actors responsible for the support and oversight of the SRM²⁰;

Upon the designation of SRM actors, they receive notification on the SRM initiation.

After the completion of the Security Risk Management assessment steps, the SRM should be discussed with members of the Security Cell. It is emphasized that the SRM assessment should not be presented to the SMT and DO without prior consultation with the security cell. At the same time DSS HQ will review the SRM assessment,

The completion of all steps in the SRM assessment is approved by the Senior Security Professional with responsibilities for the SRM.

Upon the completion of the Security Risk Management Measures step, the

¹⁷ DSS Chief Security Adviser (CSA) or Security Adviser (SA) or any other security professional designated by DSS to act in the CSA/SA capacity, such as Chief Security Officer or Chief of Security.

¹⁸ Any trained and qualified security professional, including Deputy Security Adviser (DSA), Field Security Coordination Officer (FSCO), Security Adviser) or Security Officer (SO).

¹⁹ Members of the Security Cell.

²⁰ DSS Desk Chief and Desk Officer.

SRM is subject to the review by the SMT and approval of the DO.

DSS HQ Support and Oversight. DSS HQ Desk officers will maintain oversight throughout the process in order to provide support where required or requested. In the absence of major changes in the security risk and/or programme activities DSS headquarters will endorse the SRM process once per 12 months (or more frequently if requested).

After the approval by the DO, if there are any measures that have a significant impact (e.g. continuation of activities associated with very high residual risk_ or financial implication (etc. evacuation, relocation, family duty station decision or support of a recommendation for danger pay) the SRM will be formally reviewed by DSS headquarters and endorsed by USG DSS prior to implementation.

If SRM recommends programme activities associated with very high residual security risk, the approval of PC1 activities by Executive Heads of UNSMS organizations is required before each time they are carried out.

Country Implementation. The SRM, after its endorsement by DSS headquarters, serves as MOSS and the justification for all Security Planning, which may be supported by a Local Cost Share Budget.

SRM Confidentiality

1. SRM records and documentation constitute internal UNSMS information intended only to actors of the UNSMS with security responsibilities, but not subject to publication or use by other parties outside UNSMS.
2. Handling of SRM records and documentation is subject to provisions of ST/SGB/2007/6, “Information sensitivity, classification and handling”, attached.
3. While the confidentiality of SRM records placed on e-tool will be ensured by the security of infrastructure and regulation of access rights of its users, actors of UNSMS, classification procedures and handling principles should apply to any documentation comprising sensitive information generated by the SRM process and its further distribution as per ST/SGB/2007/6.
4. Within the contents of the SRM, information deemed sensitive include the following:
 - a) Documents or information received from or sent to third parties, under an expectation of confidentiality;
 - b) Documents whose disclosure is likely to endanger the security of UNSMS personnel, assets and operations;
 - c) Any documents, if disclosure would undermine the Organization’s free and independent decision-making process;
 - d) Other kinds of information, which because of their content or the circumstances of their creation or communication must be deemed confidential.
5. SRM documentation comprising information whose unauthorized disclosure could reasonably be expected to cause damage to the work of the UNSMS shall be designated as “confidential”.
6. SRM documentation comprising information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to or impede the conduct of the work of the UNSMS shall be designated as “strictly confidential”.

Glossary

Annex A: Glossary

Security risk management	The systematic determination and implementation of timely and effective approaches for managing the effects of threats to the organisation
Threat	A potential cause of harm initiated by deliberate actions.
Hazard	A potential cause of harm resulting from non-deliberate actions.
Risk	Risk is the likelihood of a harmful event occurring and the impact of the event if it were to occur. (Risk = Likelihood x Impact)

Explaining the Condition of Risk within the SRM Process

<ul style="list-style-type: none"> • Present Risk 	The security risk based on the threats and the security measures and procedures currently in place.
<ul style="list-style-type: none"> • Projected Risk 	The expected security risk if recommended security measures and procedures were to be in place
<ul style="list-style-type: none"> • Residual risk 	The security risk remaining after approved security measures and procedures have been implemented.
<ul style="list-style-type: none"> • Risk Rating 	A rating of the risk based on an assessment of the likelihood and impact from very low to unacceptable.
Likelihood	A rating of the assessed potential for a harmful event to effect the Organization
Impact	A rating of the assessed potential harm that an event would have (if it were to occur) on the Organization.
Vulnerability	A weakness that can allow a threat or hazard to cause harm.
Vulnerable	Inadequate security risk management measures and procedures meant to address a threat
Vulnerability assessment	An assessment of whether the relevant security counter-measures are in place (strength) or absent (weakness) and the effectiveness of

	those measures.
Prevention Vulnerability	Inadequate security countermeasures meant to reduce the likelihood of an event occurring as described.
Prevention vulnerability assessment	An assessment of the degree to which the UN has implemented effective security countermeasures to lower the likelihood of the event occurring.
Mitigation vulnerability	Inadequate security countermeasures meant to reduce the impact of the event as described, if it were to occur.
Mitigation vulnerability assessment	An assessment of the degree to which the UN has implemented effective security countermeasures to lower the impact of the event if it were to occur.
Capability	The capacity or ability of threat actors to cause the threat event as described.
Intent	The motivation or disposition of a threat actor to cause the threat event as described
Event Description	Clear description of a harmful event that the SRA will examine and must include the effect on the Organization.
SRM Area	Geographic scope defined for the application of the SRM process
Programme Assessment	A process by which the security professional formally comprehends the programme requirements of UNSMS Organization.

Annex B: Programme Planning Cycle

Programme Planning Cycle

Much of the information in the Programme Assessment provided by programme managers will come from programme planning documents common to the UN system. Therefore, it is important to understand the programme planning cycle and related documents in the UN. The following paragraphs identify and summarize the key components of the planning process that contribute to the achievement of the mandates of the UNSMS organizations.

The CCA is a common instrument of the United Nations system to analyze the national development situation and identify key development issues with a focus on the MD/MDGs, and other internationally agreed development goals and treaty obligations.

The UNDAF is the strategic programme framework for the UNCT. It describes the collective response of the UNCT to the priorities in the national development framework, priorities that may have been influenced by the UNCT's analytical contribution. While specialized agencies and non-resident agencies do not use the "harmonized programme cycle" of the UNDG Executive Committee agencies, this should not be an impediment to their full engagement in the UNDAF. Prepared by UNCT in coordination with government and other stakeholders and with final government approval, outlines what each UNSMS organization plans to do in a 4 to 5 year period to assist a country to achieve some of the results of its national priority (the What and Why).

Each UNSMS organization prepares a Country Programme Document (CPD) stemming from the organization's specific Mandate and based on country priorities, MDG's and organization's Strategic Plan. The CPD is approved by each Agency Executive Board and identifies between 1 or more Outcomes (the What and Why).

The Country Programme Action Plan (CPAP) elaborates and refines the programme design and strategies as well as programme management modalities outlined in the country programme document (CPD). It provides a detailed description of the programme, its processes, the major results expected and the strategies for achieving those results. In addition, the CPAP, with detailed information on implementation modalities, constitutes the formal agreement between the UNSMS organization and the Government for implementing the country programme. The Government Coordinating Authority with overall responsibility for the country programme and the representative/ country director/ chief of operations sign the final version of the CPAP within one month of the Executive Board's approval of the country programme document. The CPAP identifies the Country Programme Outcomes (the What), Country Programme Outputs, Output indicators and Output Indicators (the How), Implementing Partners (with Who) and Indicative Resources by Output (with What Financial Resources)

Annual Work Plans (AWPs) facilitate planning and budgeting of activities to contribute to programme output(s) (as outlined in the country programme action plan (CPAP) or the global and regional action plan). The Annual Work plan (AWP) is the formal document signed by the implementing partner (IP)

and the UNSMS organization running the programme, which reflects detailed agreed activities and budgets and defines what is to be accomplished during the programme period. AWP captures the main inputs (supplies, contracts, travel, and personnel), associated resources, and their contribution to expected programme results as measured by relevant output indicators. It is the basis for requisitioning, committing and disbursing funds to carry out planned activities and for their monitoring and reporting (the What, Where, Who, and How).

Most of the information on what the UN is doing in a particular area with who, when and how is captured in the AWP. However for the purposes of the SRM this information may be too granular especially since most of these activities may be similar and conducted through many implementing partners with oversight by the UNSMS organization, usually in the form of Monitoring and Evaluation Missions, arranging meetings, conferences and training, etc. In some countries, all activities are implemented directly by either one or more UNSMS organizations. An UNSMS organization could have several hundred activities in a particular country.

Since the SRM is UN centric, the focus must be on activities implemented directly by UN personnel in a specific SRM area. Because of the large number and similarity of activities, the information may be summarized, grouping the activities together by output or outcome together with a short narrative.

It should also be noted that since the UNDAF is generally over a 4 to 5 year period. There are very little changes except in terms of AWP that are adjusted to achieve the outcomes and outputs during a particular year in the UNDAF planning cycle.

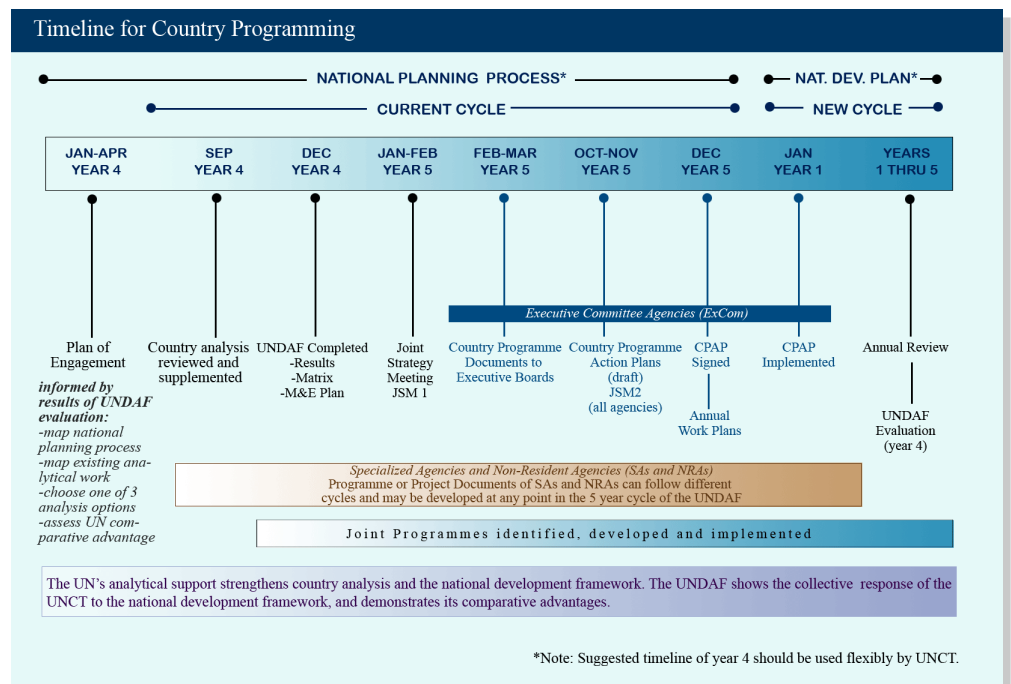


Figure 9: Timeline for Country Programming

**Annex C:
Programme
Criticality Tool**

United Nations System

Programme Criticality Framework

Document prepared by the Programme Criticality Working Group

Table of Contents

- A. Introduction
- B. Guiding Principles
- C. Overview of Programme Criticality Methodology and Criteria for Assessment
- D. Programme Criticality as part of the Security Risk Management Process
(SRM)
- E. Programme Criticality Support Structures

Annexes

Annex I: Terms of Reference of the Programme Criticality Steering Committee (PCSC)

Annex II: Terms of Reference of Executive Group on Programme Criticality (EGPC)

Introduction

1. The programme criticality framework is a common UN system framework for decision-making that puts in place guiding principles and a systematic structured approach in using programme criticality as a way to ensure that programme activities can be balanced against security risks.
2. The current document is a revision of the programme criticality framework approved by the High Level Committee on Management (HLCM) on 17 October 2011, and subsequently endorsed by the Chief Executives Board (CEB) in its autumn 2011 session. This revision is based on the lessons learned from applying the framework in a number of countries between October 2011 and December 2012.
3. Programme criticality²¹ (PC) is an important component of the United Nations Security Management System's (UNSMS) Guidelines for Acceptable Risk, approved by the CEB in April 2009²². PC is not a security function but is required for ensuring that critical programmes are implemented within levels of acceptable risk.

Guiding Principles

Applicability

4. The applicability of Programme Criticality is as defined in the UNSMS Policy Manual Chapter III: Applicability of United Nations Security Management System. A determination of programme criticality takes place through a PC assessment. Such assessments should be conducted for all activities that involve UN personnel.
5. Whilst the timing of undertaking programme criticality assessments should be determined at field level based on context and need, undertaking a UN-wide programme criticality assessment is mandatory in areas with residual risk levels of 'high' and 'very high,' as determined in the Security Risk Assessments (SRAs). A PC assessment is also beneficial when deciding how and when to undertake activities in areas where residual risk is determined to be 'medium.'

Accountability

6. Primary accountability for programme criticality is with UN senior management at the country level. The Resident Coordinator (RC) is accountable for the conduct and quality of programme criticality assessments at country level. Where there is a peacekeeping or special political mission in place, and where the Special

²¹ The concept of 'criticality' is to be understood to mean the critical impact of an activity on the population, not necessarily on the organisation.

²² CEB/2009/HLCM/INF.1

Representative of the Secretary General (SRSG)/Head of Mission has a mandate to coordinate UN activities in country, he/she has the final accountability.

7. The Designated Official (DO) is accountable to the Secretary-General, through the Under-Secretary-General for Safety and Security (USG DSS), and is responsible for the security of UN personnel, premises and assets throughout the country or designated area. The DO is responsible for ensuring that the goal of the UN Security Management System is met in his/her country or area²³. As such, the DO uses the results of the PC assessment and endorses the decisions taken at country-level, taking both the PC assessment and the SRA into consideration.

8. In areas where other UN presences/envoys or their staff are operating, all activities involving UN personnel should be part of a given PC process under the existing leadership on the ground. However, it is likely that separate PC assessments would need to be carried out for each designated area.

9. Heads of UN entities operating in country (resident and non-resident) are required to ensure that their respective entities participate in a joint UN system PC assessment and use the results in the determination of acceptable risk. Each UN entity should allocate the needed capacity to do so.

Quality assurance

10. The quality of a specific PC assessment is the responsibility of the UN leadership on the ground.

11. The Programme Criticality Steering Committee (PCSC) at HQ level is responsible for providing quality assurance of the PC framework and its implementation. This entails responsibility for oversight and review of the PC framework. In addition, the PCSC is responsible to ensure that quality PC assessments are undertaken in country areas where this is needed, and where this is not the case, take action to ensure that the assessment takes place or is revised appropriately²⁴. As part of this role, the PCSC can recommend that the EGPC be convened to make a determination on PC levels for a specific setting, as described in further detail below.

The programme criticality process

12. The determination of the criticality level for specific UN activities within a given geographic location and timeframe is termed a programme criticality assessment.

²³ United Nations Security Management System Policy Manual Chapter II: Section B Framework of Accountability for the United Nations Security Management System.

²⁴ See Terms of Reference for PCSC (annex I). Further details on the PCSC can be found in Section E below.

13. The output of the PC assessment is a list of activities determined to be within four levels of programme criticality, PC1-PC4. PC1 activities are considered most critical.

14. With the help of the PC methodology and tool (described in detail below), the UN team in country²⁵ rates which activities are PC2, PC3, PC4, and finally which are PC1. It is crucial that PC assessments are done jointly by the UN system in country as a whole and not by individual UN entities in order to provide a reality check by in-country experienced peer reviewers.

15. In identifying PC levels, the PC methodology uses existing UN planning frameworks already agreed at country level. It is thus not a planning framework.

16. The output of the PC assessment, that is the list of rated activities, along with the SRA that covers the corresponding geographic location and according to the policy for Determining Acceptable Risk, assists country level decision makers in determining which activities should be enabled based on the agreed level of acceptable risk. This helps to ensure that UN personnel do not take unnecessary risk and work on those activities that are likely to most contribute to existing UN strategic results. The framework also allows country-level programme managers to establish if programme activities or implementation modalities need to be re-designed in order to be within known acceptable risks and/or to reduce the risk.

17. In conjunction with undertaking PC assessments, the Security Management Team (SMT) must also ensure that a current SRA, outlining the residual risk levels, is in place.

Approval of programme criticality

18. Approval of levels PC1 – PC4 is given by the RC and in mission settings by the SRSG/Head of Mission as applicable, in line with the accountabilities outlined above. The final decision on which activities are enabled based on acceptable risk is with the DO²⁶.

19. In situations where an activity involving UN personnel is determined to be PC1 **and** its implementation is associated with very high levels of residual risk, the Executive Head of the relevant UN entity must certify that the activity is PC1 and that it can be implemented in situations with very high residual risk. In such cases the final approval to enable that activity in a situation of very high residual risk is given by the USG DSS.

²⁵ The DSS role in this step is a programmatic one. DSS should list the outputs/activities that it sees as important, and should not be viewing any activities listed in this step from a threat and/or risk perspective.

²⁶ See United Nations Security Management System Policy Manual Chapter II: Section B Framework of Accountability for the United Nations Security Management System.

Overview of Programme Criticality methodology and criteria for assessment

20. The PC methodology provides a structured approach to determine programme criticality. The PC tool assists in applying this structured approach.
21. A programme criticality assessment has eight steps as follows:
1. Establish geographical scope and timeframe
 2. List strategic results (SRs)
 3. List UN activities/outputs (involving UN personnel)
 4. Assess contribution to strategic results
 5. Assess likelihood of implementation
 6. Evaluate activities/outputs with PC1 criteria
 7. View PC level results, form consensus within the UN system and approve final results
 8. Agree on a process to address and manage the results of the PC assessment
22. Each step is described in further detail below. The criteria being used to assess activities/outputs are (1) Contribution to each of the SRs and (2) Likelihood of implementation. The contribution scores are averaged and multiplied by the likelihood of implementation score. The result determines the PC2-PC4 level for each of the considered activities/outputs.
23. To assist in completing the steps of a PC assessment, an excel-based tool is available. A separate PC guidance document is under development to provide further assistance and useful pointers in conducting a PC assessment.

Step 1 – Establish geographical scope and timeframe

24. The first step establishes the geographical scope/area and timeframe for the programme criticality assessment.
- The geographical scope/area of a PC assessment should be the same as the geographical area of the SRA, where possible, since this will make it easier to compare the result of the PC assessment to the residual security risk. Any differences in the areas should be noted and changes to either the PC area or an SRA area should be reflected in the next regular PC assessment.
 - As a minimum, the PC assessment must be revisited every 12 months.
 - In addition to the above, triggers for undertaking a PC assessment are changes in existing strategic plans or a significant change in the situation/programmatic conditions.
 - Since individual activities may change in importance while strategic results remain the same, a Representative of a UN entity operating in-country could flag the possible change in programmatic conditions to the UN team on the ground at any time and ask for a review of the PC assessment.
 - Scope and timeframe must be agreed before the next steps of the PC assessment are initiated.

Step 2 – List strategic results

25. The second step is to list the strategic results that the United Nations will work towards in the geographical area in the agreed timeframe.

- The SRs should be taken from the various existing planning documents that the UN system uses, such as the United Nations Development Assistance Framework (UNDAF), the Integrated Strategic Framework (ISF), the Consolidated Appeal (CAP) or other planning documents.
- The methodology allows for entering up to 6 SRs by geographical area.
- Results should be described in ‘change’ language, which describes a change in the situation of an affected population, the performance of a service, the allocation of national resources, the existence of needed policies or any other observable change.

Step 3 – List activities/outputs involving United Nations personnel

26. The third step is to enter a list of all the activities **or** outputs the UN system wishes to implement in the said geographical area and timeframe, using UN personnel.

- The UN team in country must agree in advance whether activities or outputs should be listed. Listing outputs, at the level defined in the below footnote,²⁷ is recommended rather than activities.
- If the activities/outputs do not require the presence of UN personnel to be implemented, they are not listed.
- The same list of activities/outputs should also be provided to DSS to undertake the “programme assessment” part of the SRA.
- Activities are inputs (things that we do to achieve an output) while outputs are the results we seek to achieve. Activities that are similar can be grouped together and entered once in the tool. It is important that there is agreement at the country level on whether to use outputs or activities and whether to group activities for each PC assessment so that entries are comparable.

Step 4 – Assess contribution to strategic results

27. The fourth step is to assess how each of the activities/outputs contributes to each of the strategic results.

- This assessment is on a 0-5 scale, with ‘0’ representing ‘no contribution’ and ‘5’ representing ‘very high contribution to success’. The scores for the activity’s contribution to each strategic result are averaged in the tool to get a

²⁷ ‘Outputs are changes in skills or abilities and capacities of individuals or institutions, or the availability of new products and services that result from the completion of activities within a [development] intervention *within the control of the organization*. They are achieved with the resources provided and within the time period specified’ (UNDG, Results-Based Management Handbook, 2011: <http://www.undg.org/docs/12316/UNDG-RBM%20Handbook-2012.pdf>).

score for that activity's total contribution to all the strategic results.

- It is critical that this step is undertaken by inter-agency groups to ensure peer review. The scoring is in essence relative and without having a common understanding between agencies of the scoring level comparison becomes futile.
- Before embarking on scoring all activities, a number of activities/outputs should be jointly rated by the inter-agency peer review group to set benchmarks for the scoring. This should include discussing how to score activities/outputs that can be termed as 'enablers' to programmes, such as coordination, policy/political advice, management and logistics support, etc.
- The framework does not affect UN activities implemented by third parties (government, I/NGOs, private sector, etc.) as long as such activities do not require UN personnel.

Step 5 – Assess likelihood of implementation

28. The fifth step requires the assessment of each activity/output according to its likelihood of implementation.

- This assessment is conducted using a 1-5 scale identical to the likelihood scale used in the SRA (1: very unlikely, 2: unlikely, 3: moderately likely, 4: likely and 5: very likely).
- What is being assessed is whether we have the resources and capacity to implement the activities/outputs listed within the established timeframe. We are not assessing whether the activities themselves will be successful. The question 'how do you know you can do this?' is a useful pointer in this step.
- This is a subjective assessment of relative likelihood and should be guided by such variables as acceptance by local actors, logistics, availability of personnel, funding, etc. One variable that is **not** considered in judging likelihood of implementation is the security environment, because this variable has already been taken into consideration in the SRA.
- All activities/outputs must be assessed against the same variables and these must be agreed ahead of scoring.
- The importance of this step is a reality check of the ability to implement. UN entities should be able to justify the likelihood of implementation, and therefore it is encouraged to use as verifiable criteria as possible.

Step 6 – Evaluate activities with PC1 criteria

29. The sixth step is to evaluate each activity/output to see if it meets the criteria for PC1.

- There are two possible criteria for an activity to be considered a PC1 activity:
 - a. Either the activity is assessed as lifesaving (humanitarian or non-humanitarian) at scale (defined as any activity to support processes or services, including needs assessments), that would have an immediate and significant impact on mortality; or
 - b. The activity is a directed activity that receives the endorsement of the

Office of the Secretary-General for this particular situation.

- If an activity meets either of these two criteria, it could be considered a PC1 activity and can be (but does not have to be) conducted in very high residual risk.
- Care should be taken to keep activities identified as PC1 to a minimum, because they could put UN personnel at very high residual risk.

Step 7 – View PC level results, form consensus within the UN system and approve final results

30. The seventh step is to view the PC levels of the various activities/outputs, form consensus within the UN system that this is the final rating agreed and finally approve the agreed results.

- Once agreed by the programme managers/peer reviewers, the final results must be validated by the UN team in country and approved by the RC or SRS/Head of Mission as applicable (see paragraphs 18 and 19 above).
- In the unlikely event that consensus is not reached at country level, an Executive Group on Programme Criticality (EGPC)²⁸, at USG level, can intervene to mediate and/or ultimately decide.

Step 8 – Agree on a process to address and manage the results of the PC assessment

31. The final step is to implement the results of the PC assessment. This entails using the results with the relevant SRA(s) and the policy on Determining Acceptable Risk to determine which programmes will be enabled based on an agreed level of acceptable risk. This may also include looking further into the application of risk mitigation measures for certain activities/outputs, and/or decisions on programme management. UN teams should define a process for implementation according to their contexts.

Programme Criticality as part of the SRM

32. The output of a PC assessment sits within the security management system as a core input to security decision making. It is one side of the balance when making decisions on whether a UN programme stays and delivers. The other side of the balance is the statement of the risk present at the current time, after the implementation of security risk management measures, in a specific location where the programme is being delivered; referred to as residual risk.

33. While the final decision-making on acceptable risk requires both the output of a PC assessment and determined residual risk levels, and these two components must

²⁸ See Terms of Reference for EGPC (annex II). Further details on the EGPC can be found in Section E below.

be comparable, there are clear separations in determining PC and residual risk. Accordingly, two key principles must be adhered to in order for the process to be completed correctly:

- a. Risk level has no impact on programme criticality. There must be no consideration of risk level when determining PC.
- b. Programme criticality has no impact on risk level. There must be no consideration of PC when determining risk level.

34. As outlined above, a PC assessment is undertaken by the United Nations system at country level when there is a change in existing strategic plans or a significant change in the situation/programmatic conditions, specific to a geographical location. The PC methodology and tool will be used to assign one of four programme criticality levels (PC1, PC2, PC3 or PC4) to each activity/output. A relevant SRA provides residual risk levels and suggests risk mitigation measures to lower risk. These steps form the Security Risk Management process.

35. This process will allow the principles set out in the Guidelines for Acceptable Risk to establish the maximum level of residual risk that is acceptable for a specific level of programme criticality. Figure I below depicts this relationship between programme criticality level and residual risk within the Guidelines for Acceptable Risk. Accordingly, it is permissible to implement:

- PC1 activities only in **very high** residual risk environments;
- PC1 - PC2 in **high** residual risk environments;
- PC1 - PC2 - PC3 in **medium** residual risk environments;
- PC1 - PC2 - PC3 - PC4 in **low** residual risk environments.

Of course, it is possible (and often preferable) to conduct an activity in lower residual risk, but it is not permitted to accept more risk than assigned in the Acceptable Risk Model.

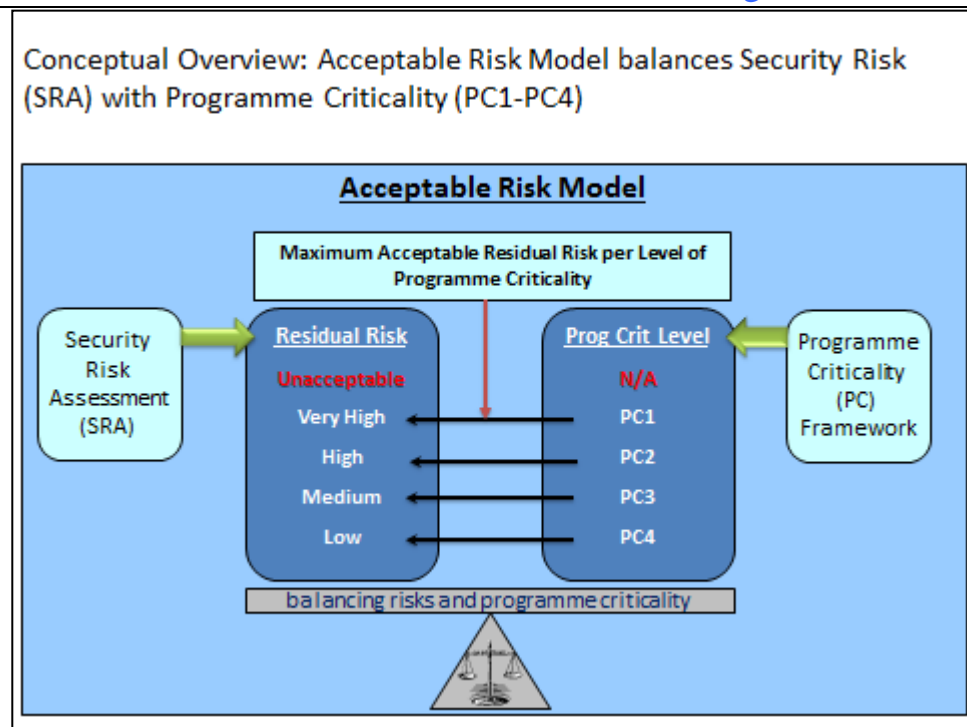


Figure 10: Balancing security risk with programme criticality

Operationalization of results

36. The output of the PC assessment will direct who, what, when and where UN programmes that require the presence of UN personnel can stay and deliver at an acceptable level of risk. While the SRA and PC processes are carried out separately, for the output of PC to be used effectively for security risk management decisions, there must be a clear statement of post security risk management residual risk to staff and programmes in every area where the programmes are to be delivered. For the Acceptable Risk Model and the PC framework to function appropriately, both residual risks and programme criticality must be realistically assessed.

37. Once the process of determining programme criticality is done, there are additional steps that need to be taken based on programme specific SRAs, as appropriate, to enable programme delivery. These steps are shown in figure II. Ultimately, together with a statement of residual risk, the PC level will inform managers in the field *what* can be delivered *where* with the presence of UN personnel. The information generated from the comparison of the PC level and the residual risk level for a specific area will thus make it possible for managers to determine programme delivery strategies, where further risk mitigation measures might be needed, possible staff deployments, etc.

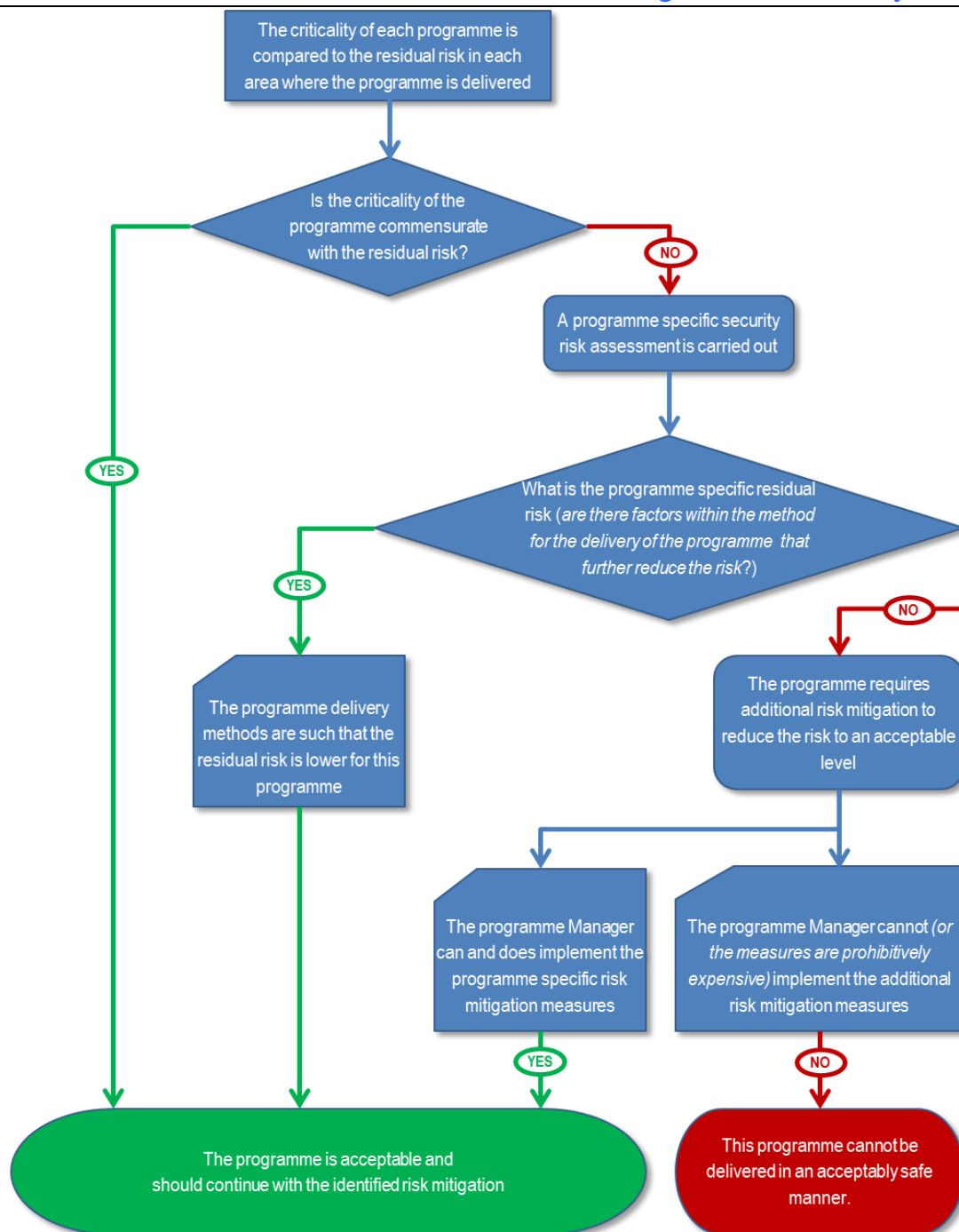


Figure 11: Security Risk Management enabling programmes

Programme Criticality Support Structures

38. The Executive Group on Programme Criticality, convened at USG level, is in place to facilitate rapid decision-making where there is an impasse and/or in the unlikely event that consensus on programme criticality levels is not reached at country level²⁹.

39. Further, in specific fast evolving crisis situations, there may be a need to rapidly

²⁹ See EGPC Terms of Reference (annex II)

make a determination of PC levels to inform decisions on how to stay and deliver. In such situations, the EGPC can be convened within 24 hours by the Chair to determine PC levels for a particular setting and timeframe. The determination of PC levels in such a situation will be made in a manner to suit the context. Where relevant, the EGPC may agree to address only those activities that are to be considered PC1, and thereafter instruct the country level leadership to undertake a PC assessment for activities of levels PC2-PC4. Decisions taken must be recorded and shared with all concerned entities. Such an EGPC meeting can be requested by any UN system entity.

40. Beyond the situations described above, the Programme Criticality Steering Committee³⁰ is the main point of contact for UN teams and senior leaders on programme criticality. The PCSC is responsible for providing quality assurance of the PC framework and its implementation. This entails responsibility for oversight and review of the PC framework. In addition, the PCSC is responsible to ensure that quality PC assessments are undertaken in country areas where this is needed, and where this is not the case, take action to ensure that the assessment in question takes place or is revised appropriately. As part of this role, the PCSC can recommend that the EGPC be convened to make a determination on PC levels for a specific setting, as described above.

41. The PCSC is supported by a technical level Programme Criticality Coordination Team (PCCT) and its Secretariat. It is envisaged that these mechanisms be dissolved once a number of agreed indicators, outlined below, are in place.

42. Indicators of success for completion of the PCSC role are:

- PC framework and guidance documents have been approved;
- PC framework has been disseminated to all UN teams on the ground;
- Briefings on PC have been held with relevant HQ fora;
- Successful completion and use of the results of a PC assessment in a significant number of countries, including in a few mission settings;
- A significant PC expert pool of UN personnel from various agencies/departments with solid knowledge of the PC framework and methodology is in place;
- Expertise on PC is maintained and mainstreamed within agencies/departments;
- Agreed plan (which is joint to the extent possible) to roll out PC and have capacity for PC individually within agencies/departments.

Validity of the PC framework

43. The PC framework will be reviewed on a biennial basis, the review to be overseen by the PCSC.

³⁰ See PCSC Terms of Reference (annex I)

Annex I:
Terms of Reference
Executive Group on Programme Criticality (EGPC)

1. The Executive Group Programme Criticality (EGPC) was established by the CEB on 28 October 2011.
2. The purpose of the EGPC is to reinforce the decision making process established through the “Programme Criticality Framework,” which is a common UN system framework and methodology to define levels of programme criticality, and thus to inform decision-making within the guidelines for acceptable risk.
2. The EGPC will have the following functions:
 - a. In the event that there is an impasse and/or lack of consensus on programme criticality levels at country level, the EGPC can either intervene to mediate or convene to determine PC levels for the specific situation in question.
 - b. In specific fast evolving crisis situations, there may be a need to rapidly facilitate a determination of PC levels to make urgent decisions about acceptable risk for UN staff. In such situations, the EGPC can be convened within 24 hours by the Chair to determine PC levels for a particular setting and timeframe. The determination of PC levels in such a situation will be made in a manner to suit the context. Where relevant, the EGPC may agree to address only those activities that are to be considered PC1, and thereafter instruct the country level leadership to undertake a PC assessment for activities of levels PC2-PC4. Decisions taken must be recorded and shared with all concerned entities.
 - c. The EGPC shall not meet or act as an appellate body.

Composition and Working Modalities

3. The EGPC shall be convened at USG level, and chaired by (TBD). This will be on bi-annual rotating basis.
4. The EGPC shall be comprised of the following organizations of the UN Security Management System: OCHA, UNDP, UNHCR, UNICEF, WFP, WHO and up to two Executive Heads of UN organisations/USGs of Secretariat Departments, ideally those with the largest operational footprint in the affected country. DSS will participate as an observer.
5. Any UN system entity can contact the Chair and request that the EGPC convenes.
6. If needed, secretariat support for the EGPC will be provided by the PCCT Secretariat. If there is no PC Secretariat in place, such functions shall be covered by the office of the EGPC Chair.

**Annex II:
Terms of Reference
Programme Criticality Steering Committee (PCSC)**

Background

1. The Programme Criticality Steering Committee (PCSC) was established by the HLCM on 7-8 March 2013 to provide oversight and quality assurance over the UN System's work on Programme Criticality, as outlined in the UN System Programme Criticality Framework.
2. The PCSC replaces the Working Group on Programme Criticality (PCWG), which was initially established by the HLCM in June 2010 to define levels of programme criticality, develop a common framework for decision making within the Guidelines for Acceptable Risk and support a roll-out of the PC framework. Following completion of the work of the PCWG, the PCSC is established to function as the main oversight body of programme criticality.

Functions

3. The PCSC is responsible to:
 - Be the main point of contact for UN teams and senior leaders on programme criticality;
 - Provide oversight of implementation of programme criticality;
 - Provide advice on the need for review of the PC Framework;
 - Provide quality assurance of the PC framework and its implementation, which entails ensuring that quality PC assessments are undertaken in country settings where this is needed, and where this is not the case, take action to ensure that the assessment in question takes place or is revised appropriately. The PCSC will not take a pro-active role in this regard, but rather respond to concerns raised.
 - As part of providing quality assurance, the PCSC can recommend that the Executive Group Programme Criticality be convened to break an impasse (see EGPC ToR for further details on the EGPC role).
4. The PCSC will provide updates on Programme Criticality to the HLCM and CEB upon request.

Composition and Working Modalities

5. The PCSC shall be convened at Director level, and chaired by [TBD]. The PCSC shall be comprised of the following organizations of the UN Security Management System: DOCO, DPA, DPKO, DSS, FAO, OCHA, UNAIDS, UNDP, UNFPA, UNHCR, UNICEF, WFP, and WHO.
6. The membership of the PCSC is open; any UN system organization can request to

become a member of the PCSC.

7. The PCSC shall convene at a minimum every 4 months. Meetings can occur as needed within these minimum intervals.

8. The PCSC is supported by a technical level Programme Criticality Coordination Team (PCCT) and its Secretariat. The PCCT is chaired at the technical level by the same organization chairing the PCSC. It is envisaged that the PCSC and PCCT will be dissolved based on the following agreed indicators:

- PC framework and guidance documents have been approved;
- PC framework has been disseminated to all UN teams on the ground;
- Briefings on PC have been held with relevant HQ fora;
- Successful completion and use of the results of a PC assessment in a significant number of countries, including in a few mission settings;
- A significant PC expert pool of UN personnel from various agencies/departments with solid knowledge of the PC framework and methodology is in place;
- Expertise on PC is maintained and mainstreamed within agencies/departments;
- Agreed plan (which is joint to the extent possible) to roll out PC and have capacity for PC individually within agencies/departments.

Annex D: General Threat Assessment Definitions and Security Levels

General Threat Assessment: Definitions and Security Levels

Part I: Definitions of Descriptors in the General Threat Assessment.

As described in Chapter 6, to ensure that the General Threat Assessment will achieve similar results when different people conduct the assessment (reliability), each category (Armed Conflict, Terrorism, Crime, Civil Unrest and Hazards) has distinct descriptors for all of the 1-5 choices for each of the three variables (Intent, Capability, Inhibiting Context, etc.).

The purpose of this part of Annex D is to provide more explanation what each descriptor means to assist in choosing the most appropriate one. Please note, however, that these guidelines are intended to assist in assigning relevant descriptors that identify the conditions on the ground which best suit the situation. They are not all inclusive, and some scope for flexibility must be given to local conditions and circumstances.

Armed Conflict: Intent

	Intent	Explanation
1	No intention to use armed / military force	External: There is no armed conflict (peace agreement in force, no territorial, political, ideological, religious disputes with neighbouring states). Internal: No organized armed group in opposition to the government.
2	Indications that military force is seen as an option or statements threatening attack but political solution still possible	External: Tension between neighbouring countries exists; politicians make threatening statements, small-scale border incidents, including harassing fire, occur. Internal: Political opposition within a state starts recruiting militants into organized armed groups and threatens the government to use force.
3	Clear statements on imminent attack and peaceful options exhausted	External: Number of border incidents increased. Politicians instigated hate media campaign. Diplomatic demarches (recall of ambassadors, breaking off of diplomatic relations) are launched. Armed forces of neighbouring countries are engaged in border conflicts, peace talks are suspended and ultimatums are issued. Internal: Organized armed groups which threatened the government to use force. Isolated guerrilla actions throughout the country occur. The government issued ultimatum to opposition and started building up forces in the area of armed opposition group operations. Small-scale engagements are possible. Cease-fire agreement is seriously challenged. Conflicting parties conduct limited-scale military operations (raids, probing actions, cordon and search operations, sporadic exchange of artillery fire and air strikes, ambushes).
4	Isolated / Limited / Sporadic armed conflict occurring	Peace talks are interrupted, ultimatum expires and war may be declared. Cease-fire agreement is broken. Part of the country may be declared independent or annexed. Conflicting parties engaged in limited-scale combined armed operations (multiple artillery and air strikes limited by area of conflict, counter-battery artillery fire, use of armour, guerrilla warfare limited by area of operations).
5	Full-scale armed conflict occurring	War or counter-guerrilla operation is occurring. The entire country/part of country is declared a war zone. All peace agreements are broken. Conflicting parties are fully engaged in armed conflict.

Armed Conflict: Capability

	Capability	Explanation
1	No or very limited presence of hostile military-type capability (no or very limited military-type weapons, training, etc.)	There is no organized armed opposition force within the country. Disorganized armed groups without coordinating structure equipped with improvised weapons and side arms. No government troops deployed (troops "in the barracks").
2	Small arms/Automatic (light) Weapons (AK47, mortars, RPG) but minimal military-type training/experience and loosely organized	This is mainly the case with internal armed conflict, when opposition is building up its armed groups both within and/or outside the country. Armed groups do not have a military-type structure or training camps, and is equipped with automatic weapons (semi-automatic rifles, submachine guns, light machine guns and grenade launchers).

3	Organized and structured forces with increased mobility and/or standoff/indirect (medium) weapon capability	Conflicting parties are in possession of heavy weapons, which are not primarily deployed outside military camps and barracks. However, some of the heavy weapons can be used for harassing fire or surge operations (air strikes and/or counter-battery fire). Armed elements may be placed at an enhanced stage of alert. Military check points and static/mobile patrols with automatic weapons may be visible in the area. Military exercises may be organized around the area. Additional manpower and materiel may be mobilized.
4	Organized and structured forces w/ HW deployed and/or large numbers of forces and intensified military operations	On-going mobilization. Heavy weapons (artillery, mortars, rocket launchers, armour, air assets and warships) and/or large number of forces are deployed to positions or at designated areas at high alert readiness. Military units are replenished and reinforced. Troops are moving towards confrontation line/area of concern, manning firing position and frequently using heavy weapons capability.
5	Organized structured forces with HW deployed or large number of forces fully engaged	Conflicting parties are engaged with full-strength armed forces (manpower and materiel), including heavy artillery, rockets, armour, air assets, warships in part of or throughout the entire country/territory.

Armed Conflict: Inhibiting Context

	Inhibiting Context	Explanation
1	Strong deterrent against initiating conflict	There is no political or social base for initiating an armed conflict. The relations with neighbouring countries and with opposition within the country are stable. Neighbouring countries are neutral or are in a political/military alliance.
2	Pressure/other incentives/agreements against hostilities	There is strong political and/or social pressure against initiating conflict. Peace/cease-fire agreements are in force and fully honoured.
3	Peace talks or unstable peace/cease-fire agreement	Peace/cease-fire agreements are unstable and seriously challenged, but political and/or social pressure on conflicting parties exists. Violations of peace/cease-fire agreements intensify. Peace talks are on-going. Special envoys and facilitators conduct missions to the area of conflict.
4	No restraint/pressure to prevent continuation or outbreak of conflict	Peace/cease-fire agreements are expired or broken at least by one conflicting party. Peace talks are interrupted. International facilitators and special envoys have left the area of conflict.
5	Armed conflict already occurring in area	Conflicting parties are fully engaged in combat.

Terrorism

The United Nations has not adopted a single definition for terrorism. For the purposes of the STA, and noting that there are numerous definitions of terrorism, an aggregate of those elements which recur most frequently have resulted in the following definition:

Terrorism is a tactic primarily used by non-state actors, which can be either an entity with no clear leadership or hierarchical organization (i.e., one that does have clear command and control), to create a psychological climate of fear within the civilian population using threats or actions in order to compensate for the legitimate political power they do not possess. It can be distinguished from guerrilla warfare, criminal abduction, or economic sabotage, although organizations that practice terror can resort to these too.

	Intent	Explanation
1	Intent to use terrorism against the UN acknowledged worldwide	The default level is the de facto “global threat of terrorism” and the fact that the UN is a named target. For the purposes of this level, generic and non-specific threats to resort to terrorism locally may also be recognised and be included at this level.

Terrorism: Intent

2	Intent to use terrorism and/or small-scale attacks	Specific warnings have been received from the host government or other member state entities indicating that terrorist acts may be under preparation. This may also include situations whereby there have been the occasional small-scale local terrorist acts with the intent to instil fear without necessarily aiming to kill.
3	Wide-spread small-scale attacks on local infrastructure	There is a local terror campaign ongoing, targeting local government institutions and public places, but not directed at the UN. Incidents are small scale, limited to small IEDs, possible abduction and targeted assassination. No VBIEDs or PBIEDs. Incidents are not mass casualty in nature. This level could also include situations where the UN has received specific information from the host government and/or member states that terrorist groups have moved from a preparedness stage to an operational stage with specific target profiles which may include the UN.
4	Sustained or large-scale attacks and/or statements or actions demonstrating intent to target UN	There is a local terror campaign on-going, targeting local government institutions and public places with intent to create mass casualty incidents. This may include the use of VBIEDs/PBIEDs and armed attacks, but also assassination, abduction and other terrorist tactics. There are express statements indicating that the UN is a target.
5	A group has already attacked the UN and is still operational in the area	There is a sustained local/regional terror campaign with the intent to cause mass casualty incidents. The use of VBIEDs/PBIEDs is common and full range of other terrorist tactics apparent, and/or a local terror campaign as per “3” or “4” above, where the UN has been attacked by the existing group or credible information suggests an attack is imminent.

Capability

Explanation

1	No known terrorist capability (threats and harassment only tactic)	There is no known capability in the region or SRM area. This level may also be assigned when there are generic but unconfirmed reports that some operatives may be apparent in the extended regional/geographic area.
2	Limited to small-scale/individual basic operations	There is limited and uncoordinated capability. Individuals operate independently with limited resources. There is minimal access to, and use of, military-type hardware and/or explosives.
3	Some isolated but coordinated operations which produce limited effects	There is now limited, but coordinated capability. Individuals operate in a coordinated fashion, with planning, guidance and/or leadership. There is still minimal access to, and use of, military-type hardware and/or explosives, and thus limited range of tactics, but can include targeted assassination and kidnapping.
4	Demonstrated capacity in wider-range and varied terror attacks	In this level there is a demonstrated ability to plan, resource and conduct small-scale coordinated attacks. This may also include the ability to deploy multiple coordinated small-scale IED operations (not suicide operations). There is evidence of access to wider range of resources.
5	Demonstrated ability in all terror tactics to produce mass destruction and/or casualties (complex attacks)	In this level there is a demonstrated ability to plan, resource and conduct complex attacks, including coordinated multiple IED, PBIED, VBIED attacks, guerrilla tactics, kidnappings and targeted assassinations. Mass casualty events are common.

Terrorism: Capability

Inhibiting Context

Explanation

1	Security forces effective	Security forces are professional, trained and effective. In the context of the country, there is no or very limited social support for the terrorist cause.
2	Security effective and/or social support of cause	The country has professional and trained security forces, but the social support network within sections of the community is apparent, limiting the capability of security forces to deter.
3	Security moderately effective and/or active assistance to terror cells in some areas	In this level the security forces are assessed to be moderately effective. This would include situations where the social support network actively assists or facilitates terror operations.
4	Security forces challenged to prevent terrorist activities	In this level security forces are challenged by the situation. Significant parts of the local community actively assist and facilitate operations. There is some freedom of movement for the operatives apparent.

Terrorism: Inhibiting Context

5	Minimal ability to deter terrorist attacks. Terrorists have safe havens	There is minimal ability to deter attacks. Operatives have established safe havens and are able to move freely throughout large areas of the country/region.
---	---	--

Crime

As much as possible, the assessment of this specific threat must be based on statistics. When statistics are not reliable or available, information must be sought from press reports, reporting of incident by UN personnel, the diplomatic community, local staff, medical and religious sources, as well as foreign travel advisories.

In addition, the way the local population protects itself can sometimes provide some useful information. The almost systematic installation of barbed wire on perimeter walls and or the recourse to private security guards can be indicators.

Crime: Intent

Intent	Explanation
1 Property crime, seldom violent	
2 Opportunistic crime against individuals, seldom violent	This variable must take into account the type of crime in order to capture the nature and dangerousness of criminal acts. It ranges from petty crimes such as ordinary theft to violent crimes which may result in the death of the victim(s). One cannot provide an exhaustive list of violent crimes, but the following criminal acts should be regarded as such: murder, assassination, kidnapping, sexual assault, assault and battery. It should be noted that in some countries or areas crimes are committed by the security forces themselves. Such crimes should be included when assessing the specific threat of crime.
3 Violent crimes focus on relatively affluent elements of the community	
4 Wide-spread violent crimes	
5 Prevalence of violence w/frequent fatalities and/or focus on the UN	

Crime: Capability

Capability	Explanation
1 Generally lone, unarmed criminals	This variable is a measurement of the dangerousness of criminals based on whether they generally operate individually, in teams or gangs and/or whether they are armed. It is obvious that an unarmed individual represents a lesser threat than a gang of armed criminals. What needs to be considered is the trend. The assessment should not be based on a one-off incident.
2 Generally lone criminals, sometimes armed	
3 Lone, armed criminals and/or unarmed criminals operating in small teams	
4 Armed criminals operating in small teams	
5 Organized, armed criminal gangs	

	Inhibiting Context	Explanation
Crime: Inhibiting Context	1	Police/criminal justice system effective and crime is socially unacceptable
	2	Crime is not socially acceptable; police/CJ system not fully effective
	3	No major social constraints on crime; police/CJ system stressed
	4	Police/CJ system significantly challenged
	5	Minimal social or Police/CJ controls on criminal activity
		This variable is a measurement of the efficiency of both law enforcement authorities and the criminal justice system in preventing, investigating crimes, arresting and prosecuting criminals. It also takes into account whether the local population tends to condone or condemn criminal activities.

Civil Unrest

Civil Unrest attempts to identify the threatening components of a deteriorating situation exemplified by the formation of public gatherings (organized demonstrations or unauthorized gatherings) which could turn violent. Experience has shown that the key components of Civil Unrest are the mood and its size. Once the crowd becomes violent, its capacity for danger increases exponentially with the introduction of weapons such as stones, machetes, petrol bombs and guns. A combination of these factors results in the degree of threat exhibited by the crowd.

	Intent	Explanation
Civil Unrest: Intent	1	Peaceful crowds only
	2	Some crowds become disruptive
	3	Crowds become violent/localized riots
	4	Extensive/wide-spread violent crowds/riots (UN possible target)
	5	Violent crowds/riots targeting UN
		Gatherings that have no stated violent intent, were not armed, were fully self-controlled and respected the attendance of crowd controlling measures.
		Gatherings began peacefully with perhaps a stated peaceful intent, but exhibited signs of aggression from individuals, small elements or organized groups. Some elements of the crowd may have resented the presence of crowd-control measures. Mood changes were evident.
		Violent behavior was clearly evident in crowds, directed at either the targeted objective of the crowd, or against the crowd-control entity. Violence included the use of improvised weapons and projectiles (stones, glass, metal, petrol bombs, locally-made weapons or conventional small arms). Localized riots with larger elements of the crowd that broke away in organized (loosely or cohesive) groups to confront the target of the crowd and/or the authority or crowd-control entity with escalating violence. The destruction of civil and private property may have been clearly evident (burning cars, breaking shop windows and looting). The mood of the crowd may have become increasingly violent and the dynamics may have change to include mob behavior and mass hysteria.
		Mass gatherings broke down into numerous crowds with violent intent, or organized crowds rioting across several different locations (but with the same purpose), which are sometimes coordinated and sometimes spontaneous. The threat from these crowds resulted from the violence and hysteria within the crowd, or from the response of the crowd control entities (which may have retaliated with the use of extreme violence). Collateral effect on UN personnel and premises ("wrong place – wrong time").
		Crowds were violent and had either been agitated to change their original purpose to then target the UN, or was formed with the intent of targeting the UN and escalated its levels of violence directing it at either UN personnel or UN property and assets.

		Capability	Explanation
Civil Unrest: Capability	1	<100 people	
	2	<500 people	As crowds increase in size they develop internal dynamics (such as mob violence and mass hysteria) which may either take on a momentum of their own and create danger to anyone present, or may be utilized by “agitators” to create a specific result. A small crowd gathered to demonstrate with peaceful intent carries relatively little threat; however, as the crowd increases in size its internal dynamics change and consequently, even without weapons, it develops a potential threat profile.
	3	<1000 people	
	4	<5000 people	
	5	5000+ people	

		Inhibiting Context	Explanation
Civil Unrest: Inhibiting Context	1	Effective crowd control or crowd self-controlled	The Inhibiting Context involves the effectiveness of the crowd-control mechanism, and this may be measured by its size and organized structure; its physical capability in terms of resources and specialist crowd-control equipment and the degree of professional training and control exhibited by the controlling force. The more resourced and effective these measures, the less likely the threat from the crowd will develop out of control. Consequently, the lowest threat comes from a small crowd with non-violent intent that is contained by effective control measures. The highest threat comes from a large crowd with violent intent (which has weapons) and which is not contained by control measures.
	2	Crowd control not fully effective	
	3	Crowd control mechanisms stressed (numbers, equipment, etc.)	
	4	Challenged crowd control mechanism or some possibly to allow anti-UN protests	
	5	Minimal crowd control mechanisms	

Non-Deliberate Events

Hazards are natural events, such as earthquakes and extreme weather or human-caused incidents such as large-scale industrial accidents, which can lead to destruction, injury or death. Although the UNSMS does not have a mandate to assess the risks posed by natural hazards, the UNSMS does have a remit to help mitigate the effects of such hazardous events, especially for crisis management and coordinating mass casualty response. Therefore, although natural hazard events will not be assessed in the Specific Threat Assessment, they are assessed in the General Threat Assessment so that the need for contingencies will be properly flagged.

Non-deliberate events are assessed using a specific set of criteria:

- History
- Intensity / Severity
- Warning / Preparedness

The precise definition of a natural disaster is an event which causes a serious disruption and is triggered by a natural hazard causing human, material, economic or environmental losses, which exceed the ability of those affected to cope. The intensity/severity of the event will be affected by the ability to effectively implement early warning and preparedness mechanisms.

A slow onset natural hazard may unfold alongside and within development processes. The hazard may be felt as an ongoing stress for a longer period of time, e.g., weeks/months, or even years. Drought is a prime example of a

natural hazard which often turns into a natural disaster by causing crops to fail, which, in turn, causes food shortages and then famines.

A rapid onset natural hazard is one which is triggered by an instantaneous shock. The impact of this hazard may unfold over the medium or longer term; an earthquake is a prime example of a sudden onset disaster.

Warning and Preparedness: The security professional should consider the regional/national/local capacity for hazard monitoring and early warning services. Is there a sound scientific basis and available capacity for making forecasts at the regional/national levels? Can accurate and timely warnings be generated locally by the national/regional/local authorities?

Part II: The General Threat Assessment and Security Levels

In addition to providing an assessment of the general threats in the SRM Area from the UN's perspective, the General Threat Assessment is also used to establish a Security Level for each SRM Area.

The General Threat Assessment and its resultant Threat Scores are not enough to establish a Security Level, because, at their most dangerous, some threat categories, such as Armed Conflict and Terrorism, are more dangerous to the UN than other threat categories at their most dangerous. Therefore, to establish a Security Level, the SRM Tool gives each threat category a different weight (sensitivity analysis) so that the resultant Security Level better reflects the reality it represents.

As noted above in Chapter 6, the General Threat Assessment achieves a Threat Score by adding the 1-5 scores of three variables (Threat: Intent, Capability and Inhibiting Context, for Hazard: History, Intensity / Severity, and Warning / Preparedness). To establish a Security Level, the SRM Tool takes this Threat Score for each of the 5 categories of threat (Armed Conflict, Terrorism, Crime, Civil Unrest and Hazard) and multiplies them by a specific weight assigned to each category. The total of the weighted scores are then compared to the standard Threat Scale to determine the Security Level.

The weights assigned to each threat category are as follows:

Threat Category	Weight
Armed Conflict	40%
Terrorism	28%
Crime	22%
Civil Unrest	8%
Hazards	2%
	100%

The following is an example of how the General Threat Assessment conducted for a specific SRM Area also assigns a Security Level to that area. The SRM Tool uses the same scale used in the General Threat Assessment above, but with the addition of a Security Level (1 to 6) as follows:

Threat Score Range	Security Level	Descriptor
3 to <5	1	Minimal
5 to <7	2	Low
7 to <9	3	Moderate
9 to <11	4	Substantial
11 to <13	5	High
13 to 15	6	Extreme

Threat Category	General Threat Assessment					Security Level	
	Intent	Capability	Inhibiting Context	Threat Score	Threat Rating	Weights	Weighted Total
Armed Conflict	2	2	1.5	5.5	Low	.4	2.2
Terrorism	2	2.5	2	6.5	Low	.28	1.8
Crime	3	3.5	2	8.5	Mod	.22	1.9
Civil Unrest	2.5	2.5	2	7	Mod	.08	.06
Hazard	History	Intensity	Preparedness	7	Mod	.02	.01
	2	3	2				
						Weighted Score	6.6
						Security Level	2 - Low

In the example above, all the numbers in blue are compared to the Threat Scale. The numbers in the General Threat Assessment get a Threat Rating. The Weighted Score gets a Security Level (in this example, Security Level 2 – Low).

