

COUNTRY SECURITY PLAN

What is it?

The Country Security Plan is more a concept than a document nowadays. Many formats exist (internet site, intranet files, mobile application, a single paper document signed by each employee, set of documents with many appendices...). Some support the idea of a single, very voluminous document per country, while others prefer sheets/checklists by theme and/or area. Whatever formula is chosen, it has advantages and disadvantages.

We will only talk here about the content and not the form, which is specific to each organisation. And the major issues at stake:

- **Creating relevant content and updating it based on a dynamic analysis**
- **Share content with the right people at the right time.**

What does it contain?

The country security plan is highly contextualized and designed to be practical, with the aim of being distributed to all staff. It includes the following:

- Distribution of responsibilities (board of directors, headquarters, country management, etc.).
- History of the conflict and key contextual issues.
- The organization's mandate and strategy in the country.
- Risk analysis (by intervention area).
- Standard Operating Procedures (risk mitigation strategies, security rules, best practices).
- Security phases and related procedures.
- Contingency plans.

The phase grid/security levels

Named a little differently depending on the organization, we often find a tool in the security plan that allows us to adapt the security management level/intensity, efforts, and tools to the evolution of certain contextual indicators. Some have evaluation matrices in Excel, others have comprehensive scoring systems. The general principle remains the same as for the grid presented here.

- **The challenge is to write varied and relevant indicators.**
- **This grid is a decision support tool, not a machine!**

Contextual changes Phase change Adapting the programme implementation Application of rules and plans of the phase			
Indicators	Phases	Programme implementation	Security management applicable procedures
Normal working conditions	PHASE 1 normal context	All areas are accessible, and the beneficiary population can receive assistance without hindrance.	The standard procedures of the organisation apply (security plan, briefings, etc.).
Increase in risk with a low operational impact	PHASE 2 tense context	Normal implementation of programmes, possibility of restricted travel depending on the zones and times.	Phase 1 in place, plus: - Quarterly review of the Risk Assessment, - Initial training all personnel on contingency plans
The security conditions no longer allow normal activities to be conducted	PHASE 3 unstable context	Potential interruption of certain activities. Possible remote management in certain zones.	Phase 2 in place, plus: - Monthly meeting with the HQ's security expert - Relocation of the families of foreign staff - Hibernation room is ready and always operational
The security of the organisation is threatened	PHASE 4 dangerous context	Suspension of the programmes. Some remote life-saving activities may be maintained.	Phase 3 in place, plus: - Non-essential staff are relocated or evacuated - Daily meeting with the HQ's security expert
The security of the organisation can no longer be guaranteed	PHASE 5 untenable context	Closing of the base (evacuation).	Phase 4 in place, plus: - Remote monitoring of the security context - Few key local admin staff working from home

The decision to escalate to a higher security phase and to de-escalate when the context improves is made by senior managers in the field or headquarters. Importantly the phases table is a decision-support tool, not a foolproof system, and should not provide a false sense of security.

Tips for writing the country safety plan

- Be concise to ease assimilation by all users.
- Write in one or more languages to be accessible to all.
- Give preference to information that can be easily updated (e.g. job titles rather than people's names).
- Guarantee confidentiality (store and disseminate thoughtfully and according to your organization's procedures).

Tips for dissemination

- Local language version.
- Each new employee is briefed during onboarding.
- One security focal point per team who ensures that everyone knows and understands the plans as well as their rights and duties regarding security.

-
- The plans are adapted to the context and applicable.
 - Shared with all personnel and accepted by employees.
 - They are concise, precise, and up to date.
-