Security risk assessments

Risk assessments are your insight into the dangers that your organisation, programmes and, crucially, your staff face in a specific location. A security risk assessment is a fundamental element of the risk management process and must be viewed as an integral part of the wider assessments involved in establishing operations or programmes in any country, whether implemented directly or by partners.

Risk analysis matrix

		Impact				
		Negligible	Minor	Moderate	Severe	Critical
Likelihood	Certain/ Imminent	🟨	🟧	🟧	🟥	🟥
	Highly likely	🟨	🟨	🟧	🟥	🟥
	Likely	🟩	🟨	🟧	🟧	🟥
	Possible	🟩	🟩	🟨	🟧	🟧
	Unlikely	🟩	🟩	🟩	🟨	🟨

🟥 Extreme risk	Immediate action required. Is the risk acceptable?
🟧 High risk	Implement specific security and safety measures and contingency plans
🟨 Medium risk	Requires heightened awareness and additional procedures
🟩 Low risk	Managed by routine security and safety procedures

A detailed understanding of the risks in a specific context is essential if your organisation is to make more informed security decisions.

Assessing risk must not be a one-off event. A continuous re-evaluation of all possible risks will help ensure that you have appropriate security measures in place at all times.

The risk assessment process first identifies the different security threats within a given context, and how your staff, assets, the programmes being implemented, or the organisation could be vulnerable. It then analyses them according to likelihood and impact to determine the degree of risk involved. Finally, it identifies and assesses the different options that could be undertaken to manage these risks. Once mitigating measures are identified it is likely there will still be some residual risk, which should be checked against your organisational risk threshold to see if it is acceptable for the programme to continue. If a risk assessment process is carried out and measures are identified but not implemented, an organisation might be exposed as breaching its duty of care.

The security risk assessment process must be documented and include key findings and proposed measures to manage the different risks. Risk assessments must also be updated on a regular basis. In addition, staff will need guidance on what the different likelihood and impact ratings mean in order to analyse more accurately the various threats and to ensure consistency throughout the organisation. For example, does 'likely to happen' mean a weekly or daily event? Furthermore, it is necessary to clarify the extent to which the predicted 'impact' considers the effect on individuals, programme activities, or the organisation as a whole, as these may be different. When considering vulnerability to threats both the specifics of the organisation and the individual should be considered. For example, role, age, gender, ethnicity, nationality and sexuality may all have an impact.

> *'Risk assessments are often perceived as an administrative burden, something to tick off the bureaucratic checklist. As a result, the vital connection between this analysis and programming is lost.'*
> ***NGO Security Advisor***

There is no prescribed format for security risk assessments but there is plenty of good practice guidance available as well as useful tools and templates. The important thing is to provide staff with a standard risk assessment template that is used in all locations, is easy to complete, and captures the essential information.

Documented risk assessments can also provide a strong rationale when requesting resources and funding to implement the security approaches and measures needed to support staff working in a specific context.

Further information

'Module 3: Risk assessment tool' in EISF guide 'Security to go'

'Security Assessment Tool' by ACT Alliance