Make Way Risk Management and Safety, Security and Safeguarding Guidance

Make Way programme Risk Working Group

1. INTRODUCTION

About this document

The aim of this document is to support civil society organisations (CSOs) to develop their safety, security and safeguarding (SSS) systems. It is important for all CSOs to have such a system in place. So, this document does not pay robust attention to how individuals can stay safe, for example. Although it does not ignore the issue; there is advice on the basic information on staying safe that organisations should communicate to their staff and other people to whom they have a duty of care. The intended reader is managers or other staff responsible for setting up an SSS within their organisation.

In this document you will find information on the elements of risk management and SSS systems. The information concerns: key concepts; principles of action; descriptions of structures to have in place. There are also has templates and tools in the annexes, which you can adapt and use in your organisation.

What are safety, security and safeguarding?

Safety and security are closely related concepts difficult to pull apart. Nevertheless, the definitions below reflect a commonly accepted distinction.

Safety refers to the condition of being free from risk or injury, e.g., from fire, health threats, car accidents. Safety can be directly influenced through preventive measures, e.g., creating a safe working environment.[1]

Security refers to the condition of being protected against threats which create risks for people.

Safeguarding refers to promoting the welfare of children and vulnerable adults and taking measures—having appropriate policies, practices and procedures in place—to protect them from any harm including physical, emotional, sexual and financial harm and neglect.[2]

2. POLICY

An SSS policy serves several functions:

1. It supports an organisation's vision for its operations.
2. It articulates to staff and others how seriously an organisation takes SSS related needs.
3. It helps an organisation be prepared for responding to SSS related needs and threats.
4. It supports implementation and operational continuity.
5. It clarifies the scope of organisational moral and legal responsibility regarding SSS.

An SSS policy document should articulate:

- The policy's objectives.
- The organisation's SSS principles.
- The organisation's scope of duty of care.
- The roles and responsibilities of the different structures and persons involved in SSS in the organisation.
- Clear guidance for compliance.

[1] https://lutheranworld.org/sites/default/files/lwf_safety_and_security_policy_-_march_2016.pdf
[2] https://www.bond.org.uk/resources-support/safeguarding/safeguarding-definitions-and-reporting-mechanisms-for-uk-ngos/#Safeguarding

All organisations should have protocols, standard operating procedures and practical tools (forms, contact information sheets) to support the organisation's staff to implement the policy and do so correctly.

3. UNDERSTANDING RISK

This section will guide you on assessing and managing risks. But, first, what is risk? **Risk refers to the possibility of actions or events, however uncertain, that could result in harm**.

An organisation may face several risks that can affect its ability to achieve programming objectives, and more seriously, can affect staff and assets. Risks can extend to other people who are not staff members but who work closely with or are connected to the organisation, e.g., consultants and volunteers, and to partner organisations (and their staff and other connected colleagues) as well as to beneficiaries of/participants in programme activities.

In the worst cases, as a result of risks people may be arrested or their lives endangered. In addition, risks can have even more harmful consequences for especially vulnerable people, such as young people with compounded vulnerabilities. Therefore, organisations should continually assess risks and communicate the level and nature of the risks to staff and relevant colleagues and partners and make informed decisions to accept or avoid these risks and take actions to mitigate them. It is important to manage safety, security and safeguarding risks actively and to make that an integral part of programme management.

Risks fall into three broad categories. Please see below.

Legal risks

CSOs may be subject to legal restrictions that can affect their operations and the work of their partners. Laws, regulations or policies may restrict the ability of CSOs to engage in certain activities, e.g., advocate for human rights, or require them to comply with disclosure or reporting requirements, e.g., declare funds from foreign organisations. In contexts where rule of law and democracy are not well and sustainably anchored[3] and CSOs are regarded as a threat to the power of autocrats, plutocrats or oligarchs, legal restrictions can change overnight. To continue to operate it is important to understand and navigate your legal framework and have a contingency plan in case your organisation is found to no longer be compliant. This could be, for example, registering ahead of time in a nearby country.

Operational risks

Organisations can be affected by various operational risks. War, natural disasters or public health crises, are common examples of unforeseen events that can pose risks to programme implementation. The COVID-19 pandemic highlighted the impact of operational risks, with activities cancelled, delayed and/or moving online.

Reputational risks

Organisations may face reputational risks, such as backlash from the public. This risk is particularly high where organisations are working on politically or socio-culturally sensitive issues, e.g., abortion. An organisation may find itself publicly lambasted in the press, on social media, on the campaign trail and/or at the pulpit. This can cause loss of constituency and funding support and demoralise and frighten staff and related colleagues and partners. It can also result in an organisation having to cancel activities or even stop operating altogether.

[3] Rule of law and democracy are not a given and are not anchored anywhere forever. As plants need water and nutrients, these elements of the social contract need constant ethical and political effort to be maintained.

Threats, vulnerabilities and capacities

To understand risk better it is also important to understand other key related concepts, like threats, vulnerabilities and capacities.

Threats
Threats are the source of a risk. These can be any form of challenge to staff, assets, an organisation, reputation or programming that exists in the context where you operate. There are *declared*, *indirect* and *incidental* threats.

- A *declared threat* is a declaration or indication of an intention to inflict damage, punish or hurt, usually in order to achieve something. Think here of hate speech directed at politicians or state-sponsored threats made to human rights defenders. Meant to intimidate, these must be taken very seriously as the persons or entities may act on their threats.
- An *indirect threat* is just that, indirect. An example is when an organisation that funds your organisation is under threat. If your partner goes out of business, you lose your source of funding.
- An *incidental threat* is a threat that results from "being in the wrong place at the wrong time". An example is finding yourself unexpectedly in the middle of a battle in an armed conflict. This could happen if rebels have moved to a new area in a very short time, surprising even the closest observers. Another common example is an unexpectedly dangerous traffic situation, e.g., all traffic lights at a very busy intersection go out in a context where traffic regulation is lax and drivers undisciplined.

It is important to examine the nature, origin, frequency and geographical concentration of threats systematically. This is called doing a *threat assessment*. Assessing threats systematically is always important, but if you are working with a group of people being targeted, such as LGBTQ+ persons in a socially and/or politically restrictive setting, it is especially important to do that often. See Annex 1 for tips on how to do a threat assessment.

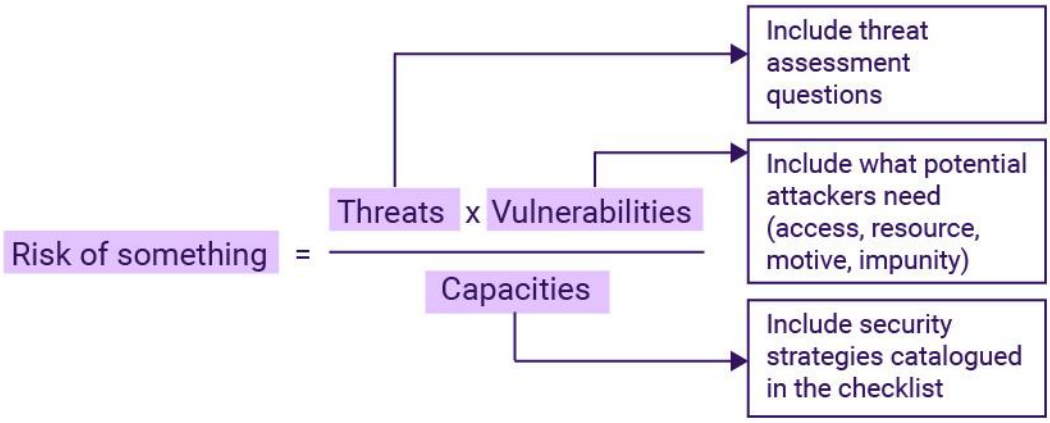
Vulnerabilities
These are the degree to which people or organisations are susceptible to a threat. This varies and changes with time. Depending on their circumstances, everyone has different levels and types of vulnerabilities. The same is true of organisations. Vulnerabilities are linked to the characteristics of a person or organisation. For example, an activist organisation operating under an authoritarian regime that publicly excoriates its president for the president's misconduct (real or not) is, all other things being equal, more vulnerable than an organisation that does not do that.

Like threats, it is important to assess vulnerabilities. A vulnerability assessment helps you to understand your organisation's exposure to threats, points of weakness and how the organisation, programmes and staff and programme participants may be affected.

Capacities
These are the strengths and resources a group or organisation can access to achieve a reasonable degree of safety and security. Examples of capacities could be having training in security or legal issues, a group working together as a team, having access to a phone and safe transportation, having access to networks of human rights defenders, etc.

Putting the concepts together
The risk formula (**Risks = Threats and Vulnerabilities / Capacities**) is the basis on which you can determine the likelihood of encountering harm.

The visual below helps show how you can structure your thinking, using the factors described above to understand risk.



4. COMPONENTS OF A RISK MANAGEMENT FRAMEWORK

Context analysis

CSOs implement their programmes in complex environments, where political decision-making processes and socio-cultural belief systems influence many actors. Many things can happen, sometimes almost simultaneously, with each event having an impact. Some consequences can amplify each other and/or compound. You need to know and understand as much as possible the context in which you are working to make informed decisions and, where possible, take pre-emptive or preventive measures.

A robust context analysis includes the following:

- Understanding of the laws, regulations and policies relevant to the work you do, issues you work on and your operations.
- Understanding of the actors or stakeholders part of or affected by your activities. Know who they are, how they interact with each other, the circumstances under which their "stake" counts, their relationships to/interest in and views on the issue(s) you work on or your activities. Also seek to understand their levels of power or influence.
- Understanding of intra- and inter-community tensions or conflicts, including historical, which could affect your work or your organisation. Know the current conflict hotspots—who is involved, including behind the scenes, who is affected, what is the geographical scope, etc.
- Understanding of the economic, political and socio-cultural factors that influence the situation of the communities you engage and your room to implement or act (civic space). Here, it is important to take into account how those factors shape the positions of power and privilege of the communities you engage. As the environment changes so will their positionality and their situations of safety and security.
- Awareness of the impact of climate collapse on the communities in your operational environment is important, paying particular attention to gendered dimensions. Consider that droughts lead to hunger which can result in more gender-based violence, intra- and inter-community conflict over natural resources and movement of people, etc.

Two methods can be used as part of a context analysis: a force field analysis and a stakeholder analysis. A force field analysis is a technique that can help you visually identify how different forces could be helping or hindering your operations. This method assumes that security problems might arise from resisting forces and that you could take advantage of some of the supporting forces. Annex 2 provides suggestions and an example for completing a force field analysis.

A stakeholder analysis maps all the relevant individual people, groups or institutions and their potential effect on your operations/operational environment based on the level of interest and influence of the different stakeholders. As part of the mapping, it is important to understand how the different stakeholders are connected–which actors are allied and which are in conflict, for example–and where interacting with one may influence relations with another. In addition, look at how your risk prevention or safety and security protection activities will affect them and their willingness to be part of your prevention or protection activities. See Annex 2 for more information.

Identifying and assessing risks

Identifying risks
After you have done your context analysis, look at what you want to achieve in a particular area and the threats in your operational context. The risks are then the potential consequences of those threats. Consider risks to funding, reputation, staff, beneficiaries and partners, material assets (office furniture, computers), and your ability to achieve your programme objectives. As part of this analysis examine your organisation's vulnerabilities, e.g., low resource capacity, office is not secure/anyone can walk in unobserved.

Likelihood and impact assessment
Once you have identified the risks you want to determine the likelihood or probability that the risks will be actualised in the form of harms (as opposed to potential risks). Of course, that does not mean you have to be a statistician to do this analysis. Some risks are very real, e.g., a meteor falling on you, but highly unlikely.[4] Other risks are very likely, for example, if you live in a normally drought-ridden, barren area, and there is heavy rain predicted, the risk of flooding is high because the ground is hard and does not absorb the water adequately.

Once you have determined the likelihood of a risk becoming a harm you can then turn to analysing the impact for each risk you identified. You can also start with the impact analysis and then determine likelihoods. There is no significant difference in the order you choose.

Gross risk
Following the risk analysis, it is important to calculate the gross risk. The gross risk reflects the combined impact and likelihood of a risk prior to any strategies, controls or actions taken to manage or measure the risk.

Residual risk
Often, no matter how many good mitigation measures you are able to develop, some residual risk will remain. For example, if you are human rights organisation implementing under a repressive government that does not have much truck with human rights, you can ensure you avoid criticising the president, secure your data according to the latest and best advice, and avoid surveillance. But the fact that you are working in a repressive context will mean that the risks you are mitigating may not be able to be mitigated fully. The remaining degree of risk is the residual risk. The residual risk reflects the ability of an organisation to address risks or lack thereof. When there is an important residual risk that is where the threshold of acceptable risk comes most into play.

[4] See this National Geographic article for a fun read on this risk.

Risk analysis at a glance

Below is common way to set up a risk analysis matrix.

GROSS RISK SCORE				
		Impact		
		Serious	Moderate	Minor
Likelihood	Likely	High	Medium	Low
	Unlikely	Medium	Low	Negligible
	Remote	Low	Negligible	Negligible

The likelihood of risks is categorised into likely (red dots); unlikely (yellow dots) and remote (green dots). The impact is categorised into: serious (red stripes); moderate (yellow stripes) and minor (green stripes).

You can also break down both likelihood and impact even more, as this model shows:

		Impact				
		Negligible	**Minor**	**Moderate**	**Severe**	**Critical**
Likelihood	**Very likely**	Low	Medium	High	Very high	Very high
	Likely	Low	Medium	High	High	Very high
	Moderately likely	Very low	Low	Medium	High	High
	Unlikely	Very low	Low	Low	Medium	Medium
	Very unlikely	Very low	Very low	Very low	Low	Low

What you choose to do will depend on how nuanced you think you need to be in your risk analysis and descriptions.

Approaches for reducing risks

Ideally, you would be able to eliminate or completely prevent a risk by removing or diminishing the threat. If that is not possible it is probably possible to reduce the risk by lowering the likelihood that the risk in question will turn into a harm. That means instead of removing the threat(s) you are reducing your exposure to the threat(s). Here are approaches you can take.

Create acceptance
This involves gaining widespread acceptance (political and social consent) in the community for your organisation's presence and activities. Building positive relationships and promoting understanding of a programme by establishing legitimacy as an impartial and independent civil society or humanitarian actor helps achieve this. Communicate this identity clearly to all parties. The success of an "acceptance approach" depends on many factors, including staff behaviour and diversity, type, design and implementation of activities, type and degree of community participation, choice of partners and how you build and maintain relationships.

Implement protection measures
Protection aims to reduce risk by reducing vulnerability. Apply protective devices/tools. Protective devices can be communications equipment, e.g., satellite phones, reliable vehicles, branding (e.g., displaying logos or not), surveillance cameras at the office, and/or protecting the perimeter of office premises. Make sure protection measures are available to all staff. Carry out training on protection measures and orient new employees regularly. For ideas and support you may find it useful to coordinate with other agencies or security forums.

Promote deterrence
Deterrence involves applying a credible counter-threat (e.g., suspension or withdrawal of activities) to contain or deter a threat and reduce risk. This approach is generally considered a last resort and is decided according to specific procedures and authorisation levels, and for most programmes, contractual agreements have clear termination clauses. The withdrawal of the programme is the main threat that can be used in an insecure area or context; however, such an action requires a high level of due diligence to address the impact on agreements with communities, beneficiaries, local authorities and/or with donors. In rare cases, legal procedures should be taken up, as in cases of fraud, theft, violence or sexual violence.

Mitigating risks

When you cannot avoid a threat or eliminate or reduce the likelihood of a risk you can seek to minimise its effects (impact). Mitigation measures are the strategies and actions you develop to minimise the impact of risks.

You looked at organisational vulnerabilities when identifying risks. In designing your mitigation measures you can also think about your organisation's strengths. For example, taking the case of flooding, perhaps your activities would not normally be able to be implemented because of flooding, but you have core funding you can use to purchase a 4x4 truck that will allow you to travel when there is flooding. As you can surmise from the example, developing mitigation measures is about leveraging or increasing strengths and adapting your activities and/or operational methods and tools.

Strategies and actions for mitigating risks
Here are some examples of strategies and actions related to types of risks.

Health related
- Have a policy on staff health that delineates your organisation's duty of care on health matters, and if possible, have a system to cover the medical costs of the people who fall under the duty of care.
- Provide advice and information to staff for avoiding risks to their health if their work heightens those risks, for example, working in areas where malaria is endemic.
- Have a policy and the tools for staff to work online when there is a dangerous epidemic.
- Allot staff sick days or personal time to go to medical appointments.
- Stimulate vaccine uptake among staff and colleagues.
- Provide staff free sanitary towels and tampons.
- Provide psychological support to staff dealing with traumatising emergencies or confronting other circumstances challenging to mental health.

Reputation related
- Ensure consistent messaging. Have a communications plan with key messages all relevant parties sign on to.
- Train staff to stick to the key messages and pitch their organisation and their work.
- Train spokespersons to work constructively with journalists.
- Develop a crisis communications plan.

Financial misconduct
- Have an anti-fraud and anti-corruption policy.
- Have a whistle-blower policy.
- Implement a code of conduct (see below).
- Adopt best practices in bookkeeping and financial management, e.g., adopting the "four eyes" principle.
- Have more than one signatory on contracts and on the organisational bank account.
- Ensure financial reports are audited through a certified accountant from a reputable firm following international standards.
- Do background checks on potential hires who will be responsible for financial management.

Sexual abuse, exploitation, abuse and harassment (SEAH)

- Have a safeguarding policy.
- Have a whistle-blower policy.
- Implement a code of conduct (see below).
- Train staff on gender equality, disability sexual orientation, gender identity and expression (SOGIE), child protection and safeguarding.
- Have an independent, external fiduciary officer people can go to safely and in confidence. See below for recommendations for having a good reporting mechanism for reporting safeguarding incidents.

Basic underpinnings for strategies and actions to mitigate risks

Here are some of the things you can do/elements you can have in place to support your strategies and actions to mitigate risks.

Address power differentials to prevent SEAH

- In the context of safeguarding, when power is abused, it can have devastating consequences. This is especially the case when working with vulnerable groups, such as young people with compounded vulnerabilities. To mitigate the risks of power differentials it is important to talk about power and address power differentials. Here are some example strategies:
- Regular outreach activities – where staff have direct meetings with a range of individuals who are representatives of a cross-section of the community –including women, men, children, older people, indigenous and minority groups, displaced people and refugees.
- Identify community representatives or groups to link with your report-handling mechanism. They can have direct contact with communities and receive and pass on any reports.
- Include women, men, children, and older people at all levels (senior, mid-career,and junior) in your staffing structure.
- Make the individual responsible for implementing and monitoring your report-handling mechanism a member of senior management.

Roll out code of conduct

As mentioned a few times, it is important to have a code of conduct. This of utmost importance especially if your organisation with working with particularly vulnerable people. It should be tailored to the context of your organisation. A basic code of conduct will include attention to:

- The importance of mutual respect between all parties involved in the work being implemented, between staff, between staff and colleagues from other organisations and between staff and community members, etc. Part of this concerns being attentive to respecting people's boundaries and treating others with dignity and with respect for their cultures and belief systems. It also about making sure staff understand their positionality and power vis-à-vis others, especially the most vulnerable.
- Online behaviour, including as regards personal attacks and divisive or inflammatory statements.
- Using mind-altering substances including medication, alcohol and street drugs while at work and/or engaging with colleagues and community members.
- Privacy rules for the management and use of personal data.
- Receiving gifts from external stakeholders or partners.
- Declaring expenses and seeking reimbursement.

This is not mean to be an exhaustive list, and there are many examples of codes of conduct available online. It is important to raise awareness of your code of conduct continuously and revisit it regularly in your organisation.

Provide basic information for staying safe
Organisations should provide advice for staying safe to their staff and other persons to whom they have a duty of care. Your SSS protocols should make sure, for example, people:

- have telephones that will work in remote areas, with solar chargers.
- a safety and security "buddy" with whom traveling staff must stay in touch regularly.
- have the names, phone numbers and email addresses of their organisation's security focal point, and other key people.
- know where they are in case laptops and phones fail, e.g., by having a geographical map of the implementation areas (ideally, plasticised).
- give you the contact information of their next of kin so you know who to contact in case of an accident.
- know where the nearest clinic or hospital is located and the emergency numbers.
- know how to respond when there is a death, and for example, a deceased colleague needs to be repatriated.
- have ready access to information on the incident reporting process.

Support staff to appreciate the impact of their personal behaviour
You should provide advice to staff and others to whom your organisation has a duty of care so they can stay safe, for example, to:

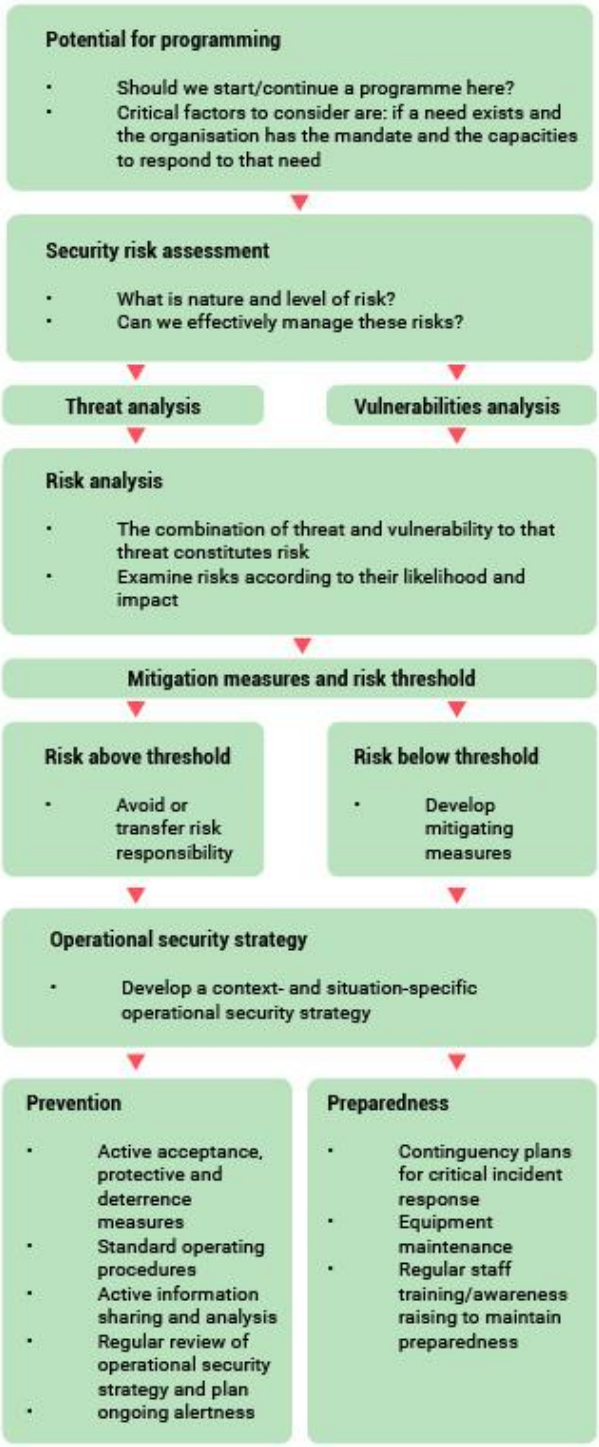
- develop a keen awareness of the environment in which they are working and their surroundings and adjust their behaviour accordingly.
- Know and be respectful of the cultural beliefs and customs of the communities your organisation engages, e.g., around drinking alcohol, dressing, religion, speaking and engaging with the opposite gender, navigating the social hierarchy, showing affection in public, etc., as per the context analysis.
- avoid language, gestures and attitudes, etc. that could offend and to communicate and interact with all individuals in a manner that is respectful and can help deescalate conflicts.
- recognise changes and danger signs before they become a threat.
- Help staff be aware and self-reflective with regard to how their position of power or lack thereof can affect how they relate to others in their work and vice versa. And help them navigate or address the power differences.

The level of detail and complexity of what to communicate depends on the nature of the activities of your organisation and the risks involved.

Security plan
Security plans are a means of putting into practice your strategies and action for responding to risks; as such they reflect how your organisation utilises acceptance, protection and deterrence strategies. Security plans should be developed for particular programme areas and should include standard operating procedures (SOPs) and contingency measures or plans for foreseeable high-impact incidents. If your risk assessment identifies a threat, the safety and security plan should advise on how to manage the risk from that threat.

Risk management framework at a glance

It may help you think through the different concepts and steps described above by looking at this visual of the elements of and process for developing your risk management framework.



Threshold of acceptable risk

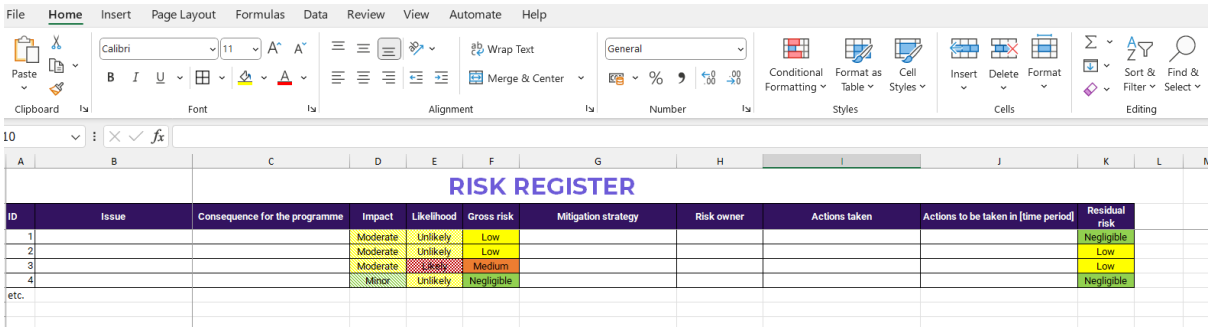
The threshold of acceptable risk is the point beyond which a risk is considered too high to continue operating. It is influenced by the likelihood that an incident will occur, the seriousness of the impact if it occurs and the ability to mitigate it. When defining the acceptable level of risk, you should consider the following:

- Is obtaining the impact of implementing the activity/programme so important that it justifies accepting such a risk?
- What would be the consequences of failing to implement the activity/programme or its interruption?
- Have all possible alternatives been explored to attain the aims of the programme?
- Has every effort, e.g., in terms of human and financial resources, been made to lower the risk?
- What strategy has been used to prevent non-eliminable risks from growing further?

Where an organisation sets the bar for the threshold of acceptable risk will all depend on the character or culture of the organisation and the organisation's priorities and risk appetite. It is important to discuss risks transparently and in a participatory manner, possibly also with the communities you engage or serve. In addition, it is particularly important to address how the risks thought to be acceptable could have implications for or an effect on vulnerable people or communities.

Monitoring risks

It is important to monitor—as well as reassess—risks regularly. The matrix showing the relationship between impact and likelihood is a basis for your risk register. The risk register is a tool you can use for risk monitoring. Here is a simple set up in Excel for a specific programme.



RISK REGISTER

ID	Issue	Consequence for the programme	Impact	Likelihood	Gross risk	Mitigation strategy	Risk owner	Actions taken	Actions to be taken in [time period]	Residual risk
1			Moderate	Unlikely	Low					Negligible
2			Moderate	Unlikely	Low					Low
3			Moderate	Likely	Medium					Low
4			Minor	Unlikely	Negligible					Negligible
etc.										

5. INCIDENT MANAGEMENT

Incident reporting and response

Responding to reports on SSS incidents is crucial. This is the case for several reasons including the following:

1. Responding to these reports can help protect the safety and wellbeing of individuals affected by the incident. This may involve providing immediate support and assistance, such as medical care or psychological support, as well as longer-term assistance, such as legal or financial aid.
2. Responding can also help prevent future incidents. By conducting thorough investigations, it is possible to identify the root causes of the incident, develop strategies for addressing these causes, and reduce the likelihood of similar incidents in the future.

3. Responding can help to maintain the trust and confidence of the community and other stakeholders. By demonstrating a commitment to addressing SSS related concerns, it is possible to demonstrate accountability and transparency and build stronger relationships with the communities where you operate.

An incident can be defined as any event or situation which could harm to a person or organisation in relation to security, safety and safeguarding. An incident can be intentionally or unintentionally provoked. The severity of each incident is defined by its impact on, and risk to, the individual(s) and the organisation.

Types of incident reports
There are typically three types of incident reports:

- An immediate incident report is sent the moment the incident begins or as soon as possible after that, often over the radio
- Follow-up incident report, giving more information as soon as this is possible
- The full incident report is sent after the incident is over. This is usually written.

Reporting and responding to incidents

Overview of the incident reporting process
The incident reporting process is a multi-stage process designed to ensure incidents are reported promptly and investigated thoroughly, with the appropriate recommendations made to prevent similar incidents from happening in the future.

What to report?
It is considered standard practice to require all incidents be reported, including if the incident merely concerns a failure on the part of staff members or others to adhere to safety, security and safeguarding procedures in the absence of an actual harm. For example, if staff members are found to be carrying out activities in high-risk areas without proper security clearance or protective gear or if they have failed to report a security incident. This means that minor incidents and near misses should be reported.

Classifying and responding to incidents
To know how to respond to incidents consistently, quickly and efficiently it is important to be able to classify them, according to their nature and severity. Below, is an example of how you can categorise incidents. You can use the analysis to define standard operating procedures for your organisation to respond to each type of incident.

It can be difficult to grade incidents, and some may fit into more than one category. If there is crossover between categories then the highest risk area should be used.

You can group incidents into three categories: safety and security; medical; and safeguarding. You can create more categories; this is just an example. In the tables below you will find a list of possible harms that can occur in each of the three respective categories mentioned above. The severity of an incident can be described as a minor incident and as a monitored, critical or crisis incident. And then there are near misses.

A minor **incident** is an event that may result in a threat to an individual and/or organisation.

A **monitored incident** is an event that results in a threat to an individual and/or organization.

A **critical incident** is an event that can result in injury or damage to an individual and/or organisation which may lead to significant harm.

A **crisis** is an event that results in substantial injury or damage to an individual and/or organisation. The event may cause significant logistical as well as psychosocial demands.

A **near miss** is an unplanned event that did not result in injury, illness, or damage to an individual or organisation, but had the potential to do so. A near miss is when harm is narrowly averted either by accident or design and can fall into any of the above incident definitions. Reporting and recording for near misses should be done in line for the type of incident so that prevention, trend analysis and future learning can take place.

The need to escalate an incident report to relevant management in your organisation goes up as you move across the colours from green to red, with green and yellow not (immediately) requiring escalation. Orange and red incidents should be addressed through urgent management responses e.g., through a crisis management team (CMT).

Please note that what follows are only examples to support your reflection process. The content is not prescriptive; it does not constitute strict instructions for how your organisation should classify and respond to incidents. Also, the meaning of terms like “moderate” and “significant” are open to interpretation. The best thing to do is to try to operationalise these terms as much as possible and be consistent in how you use them. Furthermore, when the example incidents below consider whether an alleged offender or culprit is part of the organisation in question, this has to do with the need to take additional measures, for example, to dismiss a staff person. That is a measure that will not arise with someone accused who is outside the organisation.

Whether you are obligated to respond to an incident will depend on the persons or groups of people to whom your organisation has a duty of care, which itself is a matter of policy. Often, civil society organisations define their duty of care in contractual terms, such that an organisation will have a duty of care to those individuals which whom it has a contract, e.g., staff, volunteers, interns and consultants. A contract creates a relatively clear demarcation line. But an organisation could choose to broader the scope of the duty of care to (a sub-set of) programme participants or ‘beneficiaries’, for moral reasons for instance. Note, also, how one approaches duty of care differs according to the sector. Our context here is community based organisations, non-governmental organisations and other types of CSOs doing advocacy, supporting girls to stay in school, providing youth peer counselling or doing other forms of community development. Health facilities, for example, have a duty of care to patients that will look quite different due to the nature of how health care works (there is the Hypocratic Oath, medical standards of care that apply, there are licensing requirements, etc.).

Safety and security

Incident type	Incident	Monitored incident	Critical incident	CRISIS
Arrest/detention	Staff/colleague briefly brought in for questioning and released and the case is considered “closed” by the authorities	Staff/colleague held and released but there is a risk of renewed detention	Staff/colleague held by authorities or another party with sufficient communications in place	Staff/colleague believed to be held by authorities or another party but with limited/no information available
Attack	Staff/colleague is attacked, but no injury or harm was sustained and no continued risk	Staff/colleague is attacked and sustained minor injury or harm but further risk is minimal	Staff/colleague is attacked and there is an ongoing risk of physical or other type of harm (e.g. harassment social media)	Staff/colleague is attacked and there ongoing risk of serious physical or other type of harm

Burglary/theft	Items stolen and no continued risk	Burglary takes place while staff/colleague is not at home. Items stolen and the potential is there for a similar incident to take place	Burglary takes place while staff/colleague is present and/or the theft has a wider impact, e.g., devices stolen with sensitive personal data	Items stolen have a major operational or reputational impact on people or the organisation
Robbery (threat of violence/violence used to commit theft)	Items stolen but staff/colleague is not injured and there is no continued risk	Staff/colleague is exposed to further risk from items stolen (e.g., keys, personal information) or requires counselling due to having had a traumatising experience. See "weapons" below if these were used in the incident.	Staff/colleague is injured and requires treatment at a medical facility and/or there is a continued risk which may have a major impact on people or operations. See "weapons" below if these were used in the incident.	Staff/colleague is critically injured. See "weapons" below if these were used in the incident.
Fire and smoke	Staff/colleague is not injured and there is no continued risk and there is minimal damage to property.	Fire is quickly extinguished, but some staff/colleague suffer minor injury or there is moderate damage to property	Fire is extinguished, but some people have sustained injuries and/or there was damage to property such that operations are significantly affected.	People have sustained major injuries or there has been loss of life and/or there is major impact on operations.
Kidnapping A kidnapping is never green or yellow.	ESCALATE →	ESCALATE →	Staff/colleague is released unharmed within a short time frame.	Staff/colleague is held against their will for a protracted period of time with demands in place or is injured.
Local unrest/crime	Unrest is not violent or does not affect staff or operations.	Unrest is not violent but may affect staff and operations	Unrest is/has the potential to be violent and will affect people and operations.	Unrest has a major impact on operations or there is serious injury or loss of life.
Natural disaster	Disaster does not affect staff/colleague or operations	Disaster causes staff/colleague minor injury or there is moderate damage to property	Disaster causes sustained injuries and/or there was damage to property such that operations are significantly affected.	Disaster has a major impact on operations or there is serious injury or loss of life.
Serious threat (credible threat with no physical contact)	Threat has no impact on people or operations .	Threat may have perceived impact on people or operations.	Threat impacts directly on people or operations and contingencies need to be implemented.	Threat leads to closure of operations in region/country.
Terrorism	There is a perceived threat through press, social media or other sources.	Incident takes place that is thought to be related to terrorism but this is not confirmed and there is no impact on people or operations	Incident takes place that is confirmed to be a terrorist incident and it affects operations but not people.	Incident takes place that is confirmed to be a terrorist incident and there is an impact on people and/or property.
Unexpected absence /missing person	Person absent for less than 3 hours.	Person absent and not in communication 3-6 hours.	Person absent and not in communication 6-12 hours.	Person absent and not in communication for more than 12 hours.

Weapons, exposure to	Perceived threat of exposure, e.g., through deployment of government forces	Exposure unlikely to affect staff but adds risk to operations.	Information suggesting weapons may be used or weapons pointed at or discharged in presence of staff.	Weapons discharged, injuring staff or there is loss of life.
Visa/passport not available	Visa or passport lost and can be replaced	Visa or passport lost and can be replaced with some bureaucracy.	Authorities cancel visa, seize passport to stop travel or operations.	Authorities detain travellers, see "arrest/detention".

Medical

INCIDENT TYPE	INCIDENT	MONITORED INCIDENT	CRITICAL INCIDENT	CRISIS
Illness	Staff off work for more than 3 days due to illness but no urgent evacuation or attendance at medical centre is required. Operations are not affected.	Testing and/or treatment needed at a regional medical centre or in the capital or staff is admitted to hospital. Situation where two or more staff have the same infectious illness, but duration is less than 10 days and operations are minimally affected.	Serious illness requiring treatment at medical centre of excellence. Or emergency surgery is indicated Or there is a catastrophic diagnosis received. Or there is a risk of significant disability from the illness. Situation where all or nearly all staff have the same infectious illness and it is protracted and operations are affected.	Illness cannot be stabilised or results in major disability or in loss of life.
Outbreaks	Report of outbreak in same country where staff are or in a neighbouring country where there is a real or perceived risk of spread.	Report of outbreak in same region or large city where staff/colleague is located.	Cases of disease in same specific locality as the staff/colleague.	Staff/colleague is at immediate risk due to level of threat of the outbreak or the outbreak has an impact on security.
Accident /injury	Staff/colleague has minor injuries that can be readily treated locally and there is no other harm.	Staff/colleague requires care at a regional medical centre or in the capital.	Serious injuries requiring evacuation and treatment at medical centre of excellence or emergency surgery indicated.	Accident involving major disability or loss of life.
Psychological Distress/Trauma	Staff has mental distress but feels better again after taking for ex. a couple weeks' rest	Mental distress prevents staff from carrying out regular, daily activities Not responding to supportive intervention, e.g., time off for more than two weeks and/or sessions with a psychologist.	Staff expresses suicidal ideation, has hallucinations, engaging in self-harm, and/or abusing or assaulting others Requires movement to another location or centre of excellence or removal from the programme to prevent harm to self or others.	Employee attempts suicide or significant self-harm, or harm to others.

Traffic accident	No injuries and no claims of responsibility against organisation.	Staff/colleague sustain minor injuries, able to be treated locally. Organisation's vehicles involved.	Serious injuries requiring evacuation and treatment at medical centre of excellence or emergency surgery indicated.	Staff/colleague sustain major injuries or disability or loss of life.

Safeguarding

INCIDENT TYPE	INCIDENT	MONITORED INCIDENT	CRITICAL INCIDENT	CRISIS INCIDENT
Verbal abuse	Staff/colleague expresses not being affected by incident, and no continued risk Wrongdoer is not associated with organisation.	Staff/colleague is affected by incident, is not exposed to further risk. Wrongdoer is linked to organisation.	Verbal abuse continues to pose risk to staff/colleague.	Verbal abuse causes significant (psychological or social) harm to staff/colleague.
Sexual harassment (unwelcome sexual advances without touching)	Staff/colleague expresses not being affected by incident, is not exposed to further risk Wrongdoer is not associated with organisation.	Staff/colleague is affected by incident but is not exposed to further risk Wrongdoer is linked to organisation.	Harassment continues to pose risk to staff/colleague.	Harassment continues even after perpetrator has been warned to stop Or staff/colleague is in psychological distress. See "psychological distress" above.
Sexual assault (sexual touching without consent) Sexual assault is always red.	ESCALATE →	ESCALATE →	ESCALATE →	Staff/colleague is psychologically and/or physical harmed OR is exposed to further risk.
Rape (sexual penetration without consent) Rape is always red.	ESCALATE →	ESCALATE →	ESCALATE →	Staff/colleague is raped.
Historical allegation of abuse	Claims of abuse were proven through a well-implemented (legal) investigation to have been unfounded and there have been no further complaints.	Claims of abuse were credible but not proven unfounded, and there have been no further complaints.	Claims of abuse were proven, but there have been no further complaints.	Claims of abuse were proven, there have been further complaints and there is continued risk of abuse.
Financial abuse	Staff/colleague was able to fend off the financial abuse and there is no continued risk. Wrongdoer is not associated with organisation.	Staff/colleague was not able to fend off the financial abuse. The impact is moderate but there is no continued risk. Wrongdoer is linked to organisation.	Staff/colleague was not able to fend off the financial abuse. The impact is significant but there is no continued risk.	Staff/colleague was not able to fend off the financial abuse. The impact is major and there is continued risk of financial abuse.

Abuse of power	Staff/colleague suffered no harm, and there is no continued risk. Wrongdoer is not associated with the organisation.	Staff/colleague suffered some moderate harm, but there is no continued risk. Wrongdoer is linked to organisation.	Staff/colleague suffered significant harm, but there is no continued risk.	Staff/colleague suffered major harm, and there is continued risk.
Online abuse	Staff/colleague suffered no harm, and there is no continued risk. Wrongdoer is not associated with the organisation.	Staff/colleague suffered some moderate harm, but there is no continued risk. Wrongdoer is linked to organisation.	Staff/colleague suffered significant harm, but there is no continued risk.	Staff/colleague suffered major harm, and there is continued risk.

Who to go to?
It is important to make sure it is as easy as possible for people to report incidents. This is especially the case for safeguarding purposes as the intimate nature of some violations, along with existing gender norms for example, may create a feeling of embarrassment and shame that will prevent reporting.

Security Focal Point
All organisations should have a dedicated person with the role of security focal point (SFP). The SFP is the main point of contact and is responsible for receiving incident reports. The SFP:

- initiates the administrative process for responding to reports;
- assesses the incident's type and severity (which determine the appropriate response);
- escalates incident reports to senior management or to an internal organisational SSS management committee if the organisation has such a structure;* and
- works closely with the senior management team to ensure that incidents are addressed promptly and effectively and according to the organisation's policy and relevant regulations

*When such a committee is in place, it works with the senior management team to establish and maintain policies, procedures and protocols and takes responsibility for investigating incidents and ensuring an appropriate response.

Dedicated email address
It is good practice to have a specific generic email address for incident reporting, something like "reportincidents@nameofmyngo.org". If reports go to the address of the SFP and that person is on leave or has left the organisation emails may fall through the cracks. The dedicated account for incident reporting should be able to be read by other people in case the SPF is unavailable.

Process outline
Here is what the process for incident reporting could look like. You should adapt it to your organisational context. See Annex 3 for an incident reporting format.

1. An incident has taken place and someone has submitted a report to the security focal point of the organisation through a designated email address or online form. The report should contain a detailed description of the incident, including the date, time, location, and the individuals involved, as well as relevant documentation or evidence.
2. The SFP does an initial assessment. At this early stage, the SFP may need to gather more information to complete the report. If the incident is minor, it could be sufficient to report on it in the organisation's next SSS update meeting. However, as indicated above, some incidents, like sexual touching without consent need to be escalated regardless of the SFP's own view of the severity. When in doubt the SFP should always escalate to management or the standing SSS committee if the organisation has one.

3. If an incident report is to be escalated, the SFP sends the report to the management or the SSS management committee. At this stage, the management staff in charge of handling incidents or the committee will review the incident report and determine its priority and level of urgency. This might involve considering factors such as the potential impact of the incident on the programme, the potential risks to individuals or assets, and the likelihood of similar incidents happening in the future. Based on this evaluation, the committee will determine the appropriate level of response to the incident. Here is an example of questions (not an exhaustive list) that can be used to steer an internal discussion to assess an incident, in combination with the tables above:
    - Is there a concern regarding the safety and security of staff, volunteers, or other implementers?
    - Is there a need for an emergency response to this incident?
    - Does the incident expose the implementation of activities to risk?
    - Does the incident expose the organisation to risks?
    - Is there a need to immediately report the incident to law enforcement authorities?
    - Is there the capacity to respond to the incident?
    - Can the organisational security management committee address the incident at the local level?

Time delays
The time between the receipt of the incident report and the response depends on the nature of the incident. Time delays are best determined through careful internal discussion that takes the organisation's capacity into account. A crisis incident (red colour) requires an urgent response and should be addressed immediately. A critical incident (orange colour) could be addressed within 1-2 hours of receipt of the incident report, while for a monitored incident the timeline could be within 4-6 hours of receipt of the incident report. A minor incident can wait a bit, but should be addressed within 1-2 business days from receipt of the incident report. With a near-miss it depends on the underlying conditions.

Communication of result and next steps
The decision and next steps should be communicated to all relevant parties, including the individuals involved in the incident and relevant staff and partners. If violations, e.g., of a safeguarding nature, have been confirmed:

- Report the incident to relevant authorities if required.
- Notify the individual who submitted the incident report of the decision and the next steps.
- Implement internal procedures to address the violations.
- Provide Staff/colleague -centred follow-up and support to the individuals affected by the violations.

If no violations have been found:

- Notify the individual who submitted the incident report of the decision.
- Document the incident report and decision.

Considerations related to safeguarding

As part of your handling and responding to safeguarding incident reports, it is important to:[5]

1. **Make reporting accessible and inclusive**: raise awareness of the value and importance of reporting in your organisation and with other stakeholders. Make sure it is easy to report and that there are diverse ways to receive reports (paying attention to power dynamics gender, physical or mental abilities, language, and other possible barriers) and no one is excluded from being able to report. Assess bias and social and power dynamics within your organisation and train staff and colleagues on such issues as gender equality, SOGIE and disability to reduce barriers to incident reporting.

[5] Adapted from https://www.bond.org.uk/wp-content/uploads/2022/03/bond_20_core_elements_a_toolkit_to_strengthen_safeguarding.pdf

2. **Maintain confidentiality and respect privacy**: confidentiality of all information assures the safety and wellbeing of all parties involved. It is important that individuals not fear being stigmatised by reporting on safeguarding violations. In addition, to respect privacy people should be able to report anonymously and you should have secure data management and clear and broadly communications instructions in place on if and how information can be shared.
3. **Create an environment conducive to reporting:**
    - create a safe and supportive workplace culture.
    - building trust to encourage openness about sensitive issues and being proactive and responsive about addressing safeguarding concerns.
    - raise awareness of safeguarding policies that require that all reports will be acted upon.
    - log safeguarding concerns to help identify trends for early detection of maltreatment or harm caused by staff, operations, or programmes; keep data in a secured environment.
    - display reporting pathways to demonstrate organisational commitment and increase awareness of how concerns, incidents, and reports are handled.
    - show there is no impunity for safeguarding violations in your organisation.

Handle and respond to safeguarding incidents according to the following principles:

1. **Do no harm**: assess how the incident reporting process and mechanisms your organisation has in place for reporting and responding to reports could actually make matters worse and place survivors at greater risk, and address the causal factors.
2. **Be accountable**: this means your organisation should assume responsibility for the consequences of its actions.
3. **Be transparent**: make all stakeholders aware of your organisation's safeguarding principles, plans, and resources and report back to stakeholders about the way you have handled and responded to any safeguarding reports.
4. **Be survivor-centred**: a survivor-centred approach is one where the wellbeing and the wishes of the survivor of an incident are put at the centre of all actions taken. This includes ensuring:
    - the safety and security of the survivor, any dependents, witnesses, or whistleblowers, etc.
    - assurance that issues will be handled in confidence.
    - the survivor's wishes (self-determination) and best interests are taken into account.
    - the survivor is treated with dignity and respect, demonstrating belief and trust.
    - a timely response at each stage of the process of investigation to resolution.
    - no limitations on who reports or when they report.

5. **Be impartial and just**: actions should be free of bias and should not reinforce prejudice. Disclose any conflicts of interest that may exist when handling reports. Make decisions and judgments in an objective manner, based on evidence. Treat all parties to an incident, and all those involved in the report, with dignity and full respect for their rights.

Appealing a decision made in response to an incident

Provisions for appeal

It is important to provide an opportunity for parties involved in an incident to appeal a decision. This can be done through a formal appeal process outlined in your organisation's SSS policy. An appeals process helps ensure that incidents and reports are handled fairly and transparently and that all relevant information is considered when making decisions. If an appeal is requested, you should have or set up a committee to assess the appeal and decide on the case.

Considerations for handling appeals
The following are some key elements to consider when responding to appeals:

- Accessibility: the appeal process should be easy to understand and accessible to all relevant parties.
- Timelines: the appeal process should have clear timelines for submitting appeals, responding to appeals, and making final decisions.
- Evidence-based decision-making: the appeal process should allow for the submission of additional evidence or information that may be relevant to the case.
- Fairness: the appeal process should ensure that all parties involved are treated fairly and that decisions are made objectively, without bias.
- Transparency: the appeal process should be transparent and open, and the reasoning behind decisions should be communicated clearly to all relevant parties.
- Finality: the appeal process should have a precise mechanism for reaching a final decision that is binding and cannot be appealed further.
- Record-keeping: the appeal process should have a precise mechanism for maintaining records of appeals and decisions, which can be used for future reference.

6. POST-INCIDENT

Post-incident management

Post-incident analysis
Any incident or near-incident affecting the organisation, its programmes, its partners, staff or contractors merits analysis, and a review should be standard practice. Here are key questions to guide a discussion for a post-incident analysis:

- Were security measures in place?
- Were security measures in place but not adequately communicated to staff?
- Were security measures in place and communicated but not understood?
- Were security measures in place but not followed?
- Were security measures in place and followed but inappropriate to the threat?
- Were warning signs of a specific impending threat not observed or observed but ignored?
- Were there no warning signs, and was the incident not foreseeable?
- Was the risk of a specific threat occurring accurately assessed as low, and appropriate security measures were in place, but the incident occurred anyway?
- Was the appropriate management team or committee pre-identified or pre-identified but not prepared?

It is important to consider whether there are any lessons to learn. For example:

- Should staff be better briefed?
- Should procedures be adjusted?
- Should a particular route be avoided?
- Should there be a better liaison with the police?
- Should disciplinary action be taken against any member of staff?

Consult relevant staff when considering lessons from an incident to ensure that all possible lessons are identified and that staff support the conclusions reached.

Keep records of all security incidents and analyse these occasionally. For instance:

- What do the incidents reveal about the nature of the local situation and its threats?
- Is there a pattern?
- Can any trend be discerned?
- What action should be taken as a result?

Any serious incident, whether it affects the organisation or not, should trigger a review of their threshold of acceptable risk. Key points to consider:

- Does the incident or near-incident signal that the initial analysis was flawed?
- Does it signal that the organisation has crossed the threshold of acceptable risk?
- What are the practical consequences?
- Can security measures be strengthened to reduce the risk?
- Should there be changes to the operational security strategy, and will these changes be effective?
- Should staff be relocated away from areas of high risk?

If adjustments or changes are required, staff must be assigned to implement these changes and establish a timeframe. This may require new or additional training.

Media handling after a security incident

The media may take a close interest in a security incident, mainly if it is severe. The media can sometimes impact the security of staff. By reporting details of a sensitive operation, they may arouse the anger of groups or attract the attention of hostile armed forces. Or they may simply alert criminals to the presence of high-value goods to steal. On the positive side, the media can enhance safety and security by reporting accurate information about the activities and winning local goodwill. In addition, after a security incident, the media can be used to disseminate accurate reports, thus squashing exaggerated rumours that may be circulating.

Points to consider for media relations:

- Know what message you want to convey, and ensure that you do so during the interview. Be able to express it briefly and clearly. In the Western media, getting your message in a “sound bite” of eight seconds or less dramatically increases the chances of it being broadcast.
- Ensure you always tell the truth. This is right in principle and wise in practice. It builds up a reputation for honesty, and false information is usually found.
- If you are not sure of a fact, do not publish it. If you do not know the answer to a question, say so. If you have to publish unconfirmed information, state clearly that it is unconfirmed.
- After a significant security incident, consider making an early statement to the media as soon as you have some confirmed facts. This will help to prevent false rumours from growing.
- It is not usually a good idea to say “no comment” to a question from journalists. This looks defensive and leaves an information gap they may try to fill with less reliable information.
- If you become aware of a false rumour concerning your organisation, consider how best to correct it. Assess whether it could become the cause of an increased threat to your organisation if it is left uncorrected.
- Give clear instructions to your staff on who may speak to the media and who may not. For those who are not to talk to the media, explain the reason (e.g., it helps prevent confusion if there is only one spokesperson), and let them know what they should say if approached by the media (e.g. politely refer them to the spokesperson).
- Avoid taking a defensive attitude. Journalists have a legitimate job to do and can help your operation. An ideal working relationship will be respectful and professional but not too familiar since the media may be tempted to take advantage of too close a relationship.
- Remain aware of what the local media are saying. If they use a language you do not speak, nominate a colleague who does speak the language to monitor the press and summarise it to you. This enhances your understanding of the local situation and enables you to assess the evolving security environment.
- For your own safety, avoid commenting on the government, political or military situation, especially in settings where civic space is restricted, unless there are overriding reasons to do so.

Lessons learned

A staff member should be responsible for ensuring any SSS lessons identified are fed into policies, procedures or plans as required. They should also be discussed regularly with management and programme staff so lessons are applied across programmes, as relevant.

It is important for your organisation to be self-reflective. Examine the effectiveness of your SSS management on a regular basis. Based on lessons learned, adjust your SSS management to make sure you are identifying and responding to risks and incidents in the best ways possible.

Training

Organisations should build SSS management capacity. You should provide SSS related training and professional development opportunities to staff and relevant other colleagues. Be conscious of the level and nature of SSS related knowledge, skills and competencies among staff in your organisation, and identify and address gaps. Place particular emphasis on training around SOGIE, safeguarding, adopting an intersectional lens to SSS and addressing power differentials.

Having professional SSS experts in-house is valuable for training and briefing current and future staff and other colleagues. If that is not possible you should contract external SSS trainers.

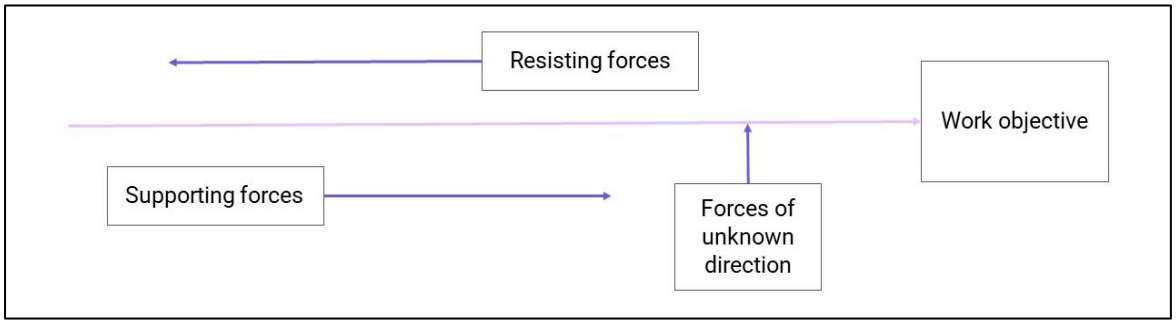
ANNEX 1: FIVE STEPS TO ASSESSING A THREAT

1. Establish the facts surrounding the threat(s). It's essential to know precisely what has happened. This can be done through interviews or by asking questions to key people, and occasionally through relevant reports.
2. Establish whether there is a pattern of threats over time. If several threats are made in a row (as often happens), it is essential to look for patterns, such as the means used to threaten, the times when threats appear, symbols, information passed on in writing or verbally, etc. Establishing such patterns is not always possible, but they are essential for a proper threat assessment.
3. Establish the objective of the threat. As a threat usually has a clear objective linked to the impact of your work, following the thread of this impact may help you establish what the threat is intended to achieve.
4. Establish the source of the threat. (This can only be done through the first three steps.) Try to be as specific as possible and distinguish between the principal and agent: for example, you could say that "the government" is threatening you. But since any government is a complex actor, it is more beneficial to determine which part of the government may be behind the threats. Actors like "security forces" and "guerrilla groups" are complex actors. Remember that even a signed threat could be false. This can be a helpful way for the person making the threats to avoid political costs and still achieve the aim of provoking fear in a defender and trying to prevent them from working.
5. Make a reasoned and reasonable conclusion about whether or not the threat can be put into action. Violence is conditional. You can never be entirely sure that a threat will – or will never - be carried out. Making predictions about violence is about stating that, given certain circumstances, a specific risk exists that a particular person or group will act violently against a particular target.

ANNEX 2: CONDUCTING A FORCE FIELD ANALYSIS

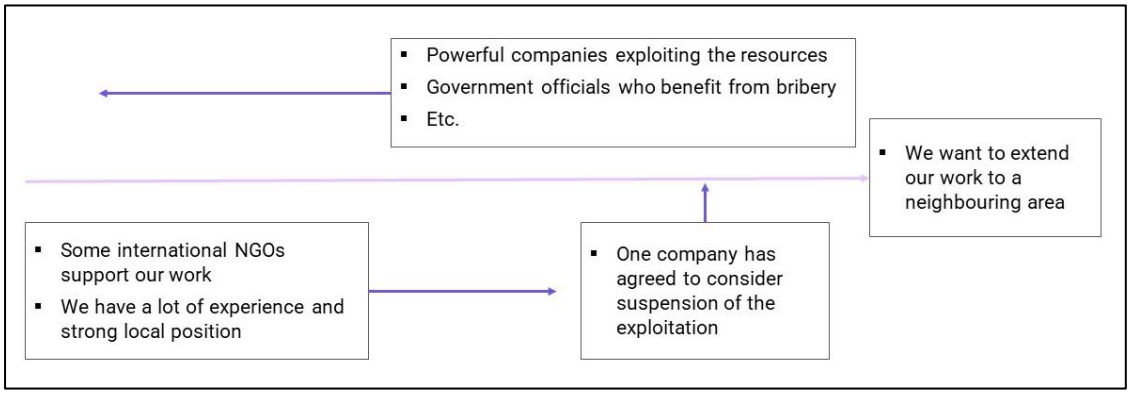
Begin by drawing a horizontal arrow pointing to a box. Write a summary of your work objective in this box. This will provide a focus for identifying supporting and resisting forces. Draw another box above the central arrow. List all potential forces preventing you from achieving your work objective here. Draw a similar box underneath the arrow containing all potential supportive forces. Draw a final box for forces whose direction is unknown or unsure.

Force field analysis for assessing the working environment



After completing your chart, start to evaluate the results. Force field analysis helps you visualise the forces you are dealing with. The goal is to find ways to reduce or eliminate the risk(s) generated by resisting forces, partly through potential help from supporting forces. Regarding the forces of unknown direction, you need to decide whether to look at them as supporting or to monitor them continuously to detect signs of their becoming either resisting or supporting.

Here is a **scenario** to help you think through a force field analysis: imagine you belong to an organisation dealing with indigenous people's rights to natural resources on their land. There are ongoing conflicts between several stakeholders about the exploitation of those resources. You now want to extend your work to a neighbouring area with similar problems.



ANNEX 3: CONDUCTING A STAKEHOLDER ANALYSIS

Stakeholder analysis in four steps:

1. Identify the broader protection issue (i.e. the security situation of human rights defenders in a given region within a country).
2. Who are the stakeholders? (Namely, which are the institutions, groups, and individuals with a responsibility or an interest in protection?) Identify and list all stakeholders relevant to that protection issue through brainstorms and discussions.
3. Investigate and analyse the stakeholders' characteristics and particular attributes, such as responsibilities in protection, the power to influence the protection situation, aims, strategies, legitimacy and interests (including the will to contribute to protection).
4. Investigate and analyse relationships between stakeholders.

After undertaking this analysis, you may wish to use a matrix like the following.

Place the list with all stakeholders relevant to a well-defined protection issue in a matrix **(see Chart 2)**: Repeat the same stakeholders' list in the first column and along the first row.

Next:
Analyse the attributes of each stakeholder (aims and interests, strategies, legitimacy and power), and fill in the boxes in the diagonal line where each stakeholder intersects with itself.
For example: Place the aims, interests and strategies of armed opposition groups in the box "A".
Analyse the relationships between stakeholders and fill in the boxes that define the most important relationships concerning the protection issue, for example, the one which intersects between the army and the United Nations High Commissioner for Refugees (UNHCR), in box "B", and so on.
After filling in the most relevant boxes, you will have a picture of the aims, strategies, and interactions among the main stakeholders concerning a given protection issue.

Chart 2: A Matrix system for stakeholder analysis

	Government	Army	Police	Armed opposition groups	National human rights NGOs	Churches	Other governments	UN agencies	International NGOs
Government	(stakeholder)								
Army		~~(stakeholder)~~						B	
Police			(stakeholder)						
Armed opposition groups				A					
National human rights NGOs					(stakeholder)				
Churches						(stakeholder)			
Other governments							(stakeholder)		
UN agencies								(stakeholder)	
International NGOs									(stakeholder)

Box "**A**"
For each stakeholder:

* aims
* strategies
* legitimacy
* power

Box "**B**"
Interrelationship between stakeholders:

(Interrelationship in relation to the protection issue and in relation to strategic issues for both stakholders)

ANNEX 3: INCIDENT REPORTING FORMAT

A standard format for an immediate incident report is as follows:

- Incident type, e.g. kidnap, death, serious assault, theft.
- Who? – who has the incident happened to?
- When? – when did the incident happen?
- Where? – where (as precisely as possible) did the incident happen?
- What has happened? What have you done about it?
- Who else is involved, what did they do, and where are they now?
- Is the situation ongoing?
- How many casualties occurred as a result, and how serious are they?
- What emergency response action has been undertaken so far? Is another response requested? If so, what?
- What help do you need?

A follow-up incident report follows the same format as the immediate report, updating information as required as soon as the situation allows. A full incident report gives a complete account of the incident and may follow a format of this kind:

- An chronological history of the incident
- Who was involved
- Reasons for any decisions taken
- Lessons to learn from the incident
- Identification of any failure of procedures or staff and recommendations for any remedial or disciplinary action

Include the date, author, the role of the author (involved in the incident or not?) and signature. Unfortunately, the date and author's name are often omitted by report writers, which causes problems if there are any queries concerning the incident.