Image not found or type unknown

Introduction to risk assessment [starter activity]

image-1605640366569.png
Image not found or type unknown

This activity is designed to introduce and exercise a framework for doing risk assessment.

Learning objectives

Learning objectives this activity responds to:

- Understanding the concepts that underlie risk assessment.
- Beginning to apply a risk assessment framework on their personal and/or organisational security.

Who is this activity for?

This activity is designed for participants who have basic or no experience of risk assessment. It is also designed for a workshop with participants from different organisations.

Time required

Realistically, this activity requires a day (eight hours, minimum) to do properly.

Resources

- Flip chart paper and markers
- Projector
- Laptops.

Mechanics

For this activity, create a scenario of an individual or group that the participants can practice doing a risk assessment on.

Depending on your participants, some options can be:

- A human rights group in a country that just passed a law to monitor NGOs
- A transwoman launching a website to support other transwomen
- A network of women's rights advocates working on an issue that is considered taboo in their countries
- A group with a safe house for young transpeople
- A small LGBTIQ group under attack online
- A queer woman from a racial minority group posting their opinions online.

Break the participants down into groups. They can work on the same kind of organisation/group or work on different kinds of organisation.

> **Facilitation note:** It is important here that the scenario resonates with the participants and that it is close to their experience.

Once everyone is in their groups, present the Basic risk assessment presentation.

Group work 1: Flesh out context and scenario

Before the groups can begin filling out the Risk assessment template, they should flesh out their chosen scenario.

For a group scenario:

- Create a profile for this organisation: location, size of the organisation, general mission of the organisation.
- Name their activities, or changes in their context, that put them at risk – this could be a new law, or they're planning an activity that their detractors will want to interrupt. This could also be an internal shift that might present risks – e.g. a recent conflict within an organisation – or an external event that is causing significant internal stress among members of the organisation.
- Name who will be hostile to their actions, and who their allies are.

For an individual scenario:

- Create a profile for this individual: age, location, sexual orientation, how active they are on social media.
- Create the opinion they are being attacked for. Or describe the website they are creating that puts them at risk. Or the context situation that creates a vulnerable situation (e.g. being thrown out of their home, leaving an abusive relationship with someone in the same organisation or movement, etc.).
- Name who will be hostile to their actions, and who will support them.

Give each group an hour to do this.

Afterwards, have each group present their scenarios quickly.

Then present the Risk assessment template.

Some notes about the table:

- Threats should be **specific** – what is the threat (negative intention towards the individual group) and who is threatening them?
- Think about **probability** of a threat in three layers:
  - Vulnerability – what are the processes, activities and behaviours of the individual or the group that increases the likelihood of the threat becoming real?
  - Capacity of the people/person doing the threatening – who is making the threat and what can they do to enact it?
  - Known incidents – has a similar threat been made with a similar scenario? If the answer is yes, then the probability increases.
- In thinking about **impact**, consider not just the individual impact, but the impact on a greater community.
- Assessing low/medium/high probability and impact will always be relative. But this is important to do in order to prioritise what risks to make mitigation plans for.
- Risk – this is a statement that contains the threat and the probability of it.

Group work 2: Risk assessment

Using the risk assessment template, each group analyses the risks in their scenario. The task here is to identify different risks, and analyse each one.

> **Facilitation note:** Give each group a soft copy of the risk assessment template so they can document their discussions directly on it.

This group work will take at least two hours, with the trainer-facilitator consulting with each group throughout.

At the end of this, debrief with the groups by asking process questions rather than getting them to report back on their templates:

- What difficulties did your group have in assessing the risks?
- What were the main threats that you identified?
- What were the challenges in analysing probability?

Mitigation tactics input and discussion

Using the text for a presentation on mitigation tactics (see the Presentation section), present the main points and have a discussion with the participants.

Group work 3: Mitigation planning

Ask each group to identify a risk that is high probability and high impact. Then ask them to create a mitigation plan for this risk.

Guide questions

Preventive strategies

- What actions and capacities do you already have in order to avoid this threat?
- What actions will you take in order to prevent this threat from being realised? How will you change the processes in the network in order to prevent this threat from happening?
- Are there policies and procedures you need to create in order to do this?
- What skills will you need in order to avoid this threat?

Incident response

- What will you do when this threat is realised? What are the steps that you will take when this happens?
- How will you minimise the severity of the impact of this threat?
- What skills do you need in order to take the steps necessary to respond to this threat?

This group work will take about 45 minutes to an hour.

Afterwards, debrief by asking about the process and questions they have about the activities they have gone through.

To synthesise this learning activity, reiterate some lessons:

- Risk assessment is useful to come up with realistic strategies (preventive and responsive).
- Focus on the threats that have a high probability of being realised, and the ones with high impact.
- Risk assessment takes practice.

Presentation

There are three things to present in this activity:

- The basic risk assessment presentation
- The risk assessment template
- The mitigation tactics input (see text below).

Text for presentation on mitigation tactics

There are five general ways to mitigate risks:

Accept the risk and make contingency plans

Contingency planning is about imagining the risk and the worst case impact happening, and taking steps to deal with it.

Avoid the risk

Decrease your vulnerabilities. What skills will you need? What behavioural changes will you have to undertake to avoid the risk?

Control the risk

Decrease the severity of the impact. Focus on the impact and not the threat, and work towards minimising the impact. What skills will you need to address the impact?

Transfer the risk

Get an outside resource to assume the risk and its impact.

Monitor the risk for changes in probability and impact

This is generally for low-probability risks.

There are two ways to look at dealing with risks

Preventive strategies

- What actions and capacities do you already have in order to avoid this threat?

- What actions will you take in order to prevent this threat from being realised? How will you change the processes in the network in order to keep it from happening?
- Are there policies and procedures you need to create in order to do this?
- What skills will you need in order to prevent this threat from being realised?

Incident response

- What will you do when this threat is realised? What are the steps that you will take when this happens?
- How will you minimise the severity of the impact of this threat?
- What skills do you need in order to take the steps necessary to respond to this threat?

Adjustments for an organisational workshop

This activity can be used in a workshop context where the risk assessment is being done by an organisation, and the role of the trainer-facilitator is to guide the organisation through the process.

In order to do this, instead of fleshing out the scenario, have a discussion on the general threats that the organisation is facing. This could be a change in law or government that has implications on the organisation's ability to continue its work. It could also be a specific incident when the people in the organisation felt that they were at risk (for example, a partner organisation discovering they are being surveilled, or the organisation itself being monitored). Follow that up with a discussion on what capacities the organisation already has – resources, connections, supporters and allies, and skills. Grounding a risk assessment activity by building common knowledge about the threats the organisation is facing and its capacities will be important for the rest of the process.

Break the participants up by team/unit as they go through the risk assessment template.
In this context, the mitigation planning is as important as the risk assessment template, so both areas will have to have equal time.

For an organisational context, this activity may take up to two days, depending on the size of the organisation and its operations.

Further reading (optional)

- Risk assessment basics
- Risk assessment in movement organising

image-1605451879726.png

Revision #7

Created 18 April 2023 02:37:49 by Kira

Updated 28 July 2023 14:51:36 by Kira