RISK MITIGATION 101

RESOURCE KIT TO HOLISTICALLY ADDRESS RISKS

Table of Contents

Introduction

Welcome to this **Risk Mitigation 101** resource kit. This guide aims to provide you with key knowledge, skills, and practical steps to help you identify, assess, and develop steps to address risks you or your organization might face. Whether you are a journalist, a social communicator, media outlet, or civil society organization, this kit is designed to provide you with the basic tools and strategies needed to navigate risk scenarios proactively or reactively.

You may have received this resource kit after having reached out to the Risk Support Network to request risk mitigation support, or you may have received it elsewhere but, following reading through this document, you may decide to reach out to us for additional risk mitigation support. Please do not hesitate to do so. Either way, this guide is intended as complementary to more in-depth and tailored support by the Risk Support Network, introducing key concepts and basic steps you can take to assess, map, and address risks independently.

The Risk Mitigation 101 resource kit is designed to be both informative and actionable. Each section builds on each other, taking you through the process of understanding risks, conducting risk assessments, and implementing risk mitigation steps. Additionally, you will find links to additional readings and other organizations that might be able to provide support tailored to your needs. We encourage you to actively engage with the kit's content and adapt the proposed strategies and steps to your unique needs. We also welcome any feedback that you might have on the information provided in this document.

If you are in a **medical emergency** or if you or someone you know is experiencing an **acute emotional crisis**, please call your local emergency number (if available and safe) or contact an international crisis hotline that serves individuals in your country. You can find a comprehensive list of available crisis hotline services, listed by country, here (list of international suicide hotlines by Open Counseling). If you are interested in more immediate steps to address risks you might face, jump straight to the section "Immediate risk mitigation steps" for some suggestion on how to address common risks.

The Foundation: Understanding Risks

What are risks

In the first part of this resource kit, we will discuss the concepts of risks, threats, and vulnerabilities.

A **threat** is anything that has the potential to cause harm or loss. This can include natural disasters, accidents, or malicious actions taken by individuals or groups.

Vulnerability refers to the likelihood or probability of being confronted with a threat, as well as the potential consequence or impact if or when that threat materializes. Vulnerability can vary depending on a variety of factors, including the location, resources, and resilience of an individual or community.

Risk is a measure of vulnerability to threats in the environment. It is determined by the likelihood and potential impact of a threat as well as the level of vulnerability to that threat. By understanding and managing risks, we can take proactive steps to reduce our vulnerability and protect ourselves and those around us.

Vulnerabilities can be treated by identifying and addressing weaknesses or areas of vulnerability. We can proactively take measures to correct them and reduce our overall level of vulnerability. It is important to regularly assess and address vulnerabilities in order to maintain our safety and well-being.

Threats can generally be identified but not controlled. While we can take steps to mitigate the risks posed by threats, we cannot completely eliminate the threat itself. For example, we can take precautions to reduce the risk of being affected by a natural disaster, but we cannot prevent the disaster from occurring. Threats need to be identified, but they often remain outside of our control.

Risks, on the other hand, can be identified and mitigated. This is why risk assessments are so important for protecting ourselves and those around us from potential harm or loss. However, the goal of managing and mitigating risks isn't typically to eliminate them entirely, since this is often impossible. Instead, the focus is on understanding the risks, determining which ones are most likely to happen and could cause the most harm, and taking steps to address those first.

Types of risks

Risks can be related to different aspects of your overall safety, such as your physical, digital, and psychosocial safety. However, it is important to understand that risks are typically not isolated. Rather, they often overlap and are interconnected. For instance, a physical safety risk, such as a violent attack

or harassment, might be accompanied by digital risks, such as hacking, online threats, or unauthorized access to your data. Similarly, psychosocial risks, such as burnout or anxiety, may become even more severe when physical or digital threats become overwhelming. By identifying and assessing risks holistically, looking at all areas of your life or your organization's operations, we can better protect our well-being and resilience. Find below a list of some common risks faced by individuals and organizations in your line of work:

Physical safety risks	Digital safety risks	Psychosocial safety risks
• Targeted violence or harassment • Surveillance and stalking • Kidnapping • Detention or arrest • Violent confrontations • Risks related to natural disasters • Risks related to operating in violent conflict zones • Office break-ins • Vandalism	• Hacking • Data theft • Phishing and malware attacks • Surveillance and digital monitoring • Doxxing • Online harassment • Device confiscation or theft	• Burnout • Stress • Anxiety • Post-Traumatic Stress Disorder (PTSD) • Harassment and online abuse • Vicarious trauma

Conducting a Risk Assessment

Overview of risk assessments

In conducting a risk assessment, you will typically follow five consecutive steps. In the following section, you will find additional information on how to conduct each of the five steps of risks assessments. The five steps of a risk assessment are:

1. **Identify** (or map) all **risks** that may cause harm and negatively affect our work.
2. **Analyze** the **risks** and determine their likelihood and consequences to get a better understanding of the risks you face and be aware of their potential impact.
3. **Rank** the detected **risks** according to their potential impact. Some risks may have such a huge potential negative impact that it is not worth the risk while the impact of other risks may be small.
4. **Plan** your **response** to the risks. Starting with the highest level of risk, the goal is to develop a plan that makes it possible to reduce the likelihood and impact of risks. Because risks are variable, it is essential that the risk assessment be reviewed and updated regularly to maintain its relevance and usefulness.
5. **Develop mitigation strategies** to reduce the likelihood or impact of the more severe risks.

Mapping and categorizing risks

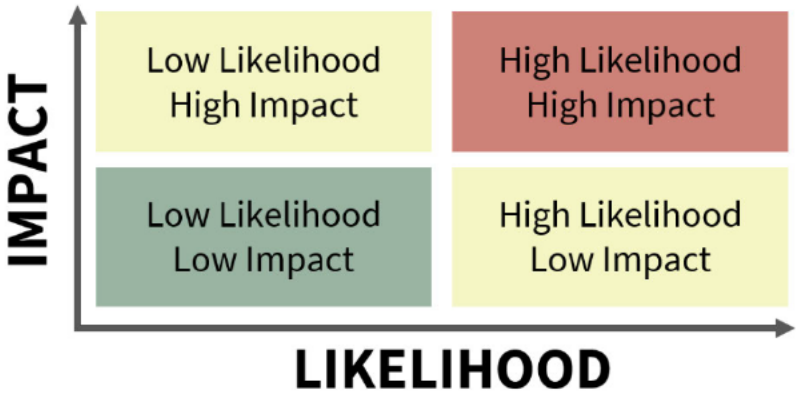
Mapping risks is a vital step in the risk assessment process. It allows you to get a better understanding of the risks you or your organization might be facing, to visually represent and organize them, as well as to identify their potential impacts and how they might relate to one another. This process not only helps you clarify complex risk scenarios, but also makes it easier to prioritize which risk(s) to address first. If you feel comfortable with it, consider doing the risk mapping with a trusted individual, e.g. a colleague or friend, who can provide additional information, assist in analyzing potential risks, and offer emotional support throughout the process.

To start, come up with a list of all the risks you or your organization are facing in your current situation or might face in the future. Think of different kinds of risks that are relevant to your physical safety, digital security, and psychosocial well-being, as well as risks specific to your identity or your organization's profile. Remember to think holistically about your risk situation and how different risks

might relate to each other. Refer to the "Types of Risks" section in this document for some common risks individuals and organizations in your line of work might face.

Once you have compiled a list of current and potential future risks, it is important to consider both the likelihood of the risks occurring and their potential impact on you or your organization. Some risks may have a high likelihood of occurring but may not have a significant impact, while others may have a low likelihood of occurring but could have a significant impact if they do. When thinking about a risk's likelihood, consider factors such as historical occurences, frequency of similar incidents, and emerging trends in your operating environment. When trying to assess a risk's impact, try to locate them on a scale from minimal impact (e.g. minimal disruption to your work life or safety, minor costs) to high impact (e.g. loss of life, destruction of critical equipment, severe damage).

Mapping out potential risks on a likelihood-impact graph can help you visualize which risks are most pressing and require immediate attention. Once you have mapped and categorized risks by their likelihood impact, place them on the Likelihood-Impact Graph below.



The graph is divided into four main quadrants:

- High Likelihood/High Impact: These are high-priority risks. They typically require immediate attention, as they pose the most serious risks to you or your organization.
- High Likelihood/Low Impact: These risks are frequent but less serious. You or your organization should monitor them closely but would typically prioritize resources and time for the risks with the highest potential impact.
- Low Likelihood/High Impact: These are rare but dangerous risks. Even if they are unlikely to occur, you or your organization should develop contingency plans or Standard Operating Procedures (SOPs) to be able to address them, should they in fact materialize.
- Low Likelihood/Low Impact: These risks are minor and infrequent. They can often be deprioritized but should be continuously monitored.

It is especially important to pay attention to risks that fall into the High Likelihood/High Impact quadrant, as these are the risks that have the greatest potential to harm you or those around you. These

are the risks that you should prioritize in terms of creating mitigation strategies to address them. By focusing on these high-impact, high-likelihood risks, you can better protect yourself from harm.

Additionally, you should routinely review and, if needed, update your risk mapping since likelihoods and impacts can evolve over time. This ensures that your risk mapping remains relevant and up-to-date and allows you to adjust your risk mitigation plan as needed.

Please see the "Risk Mapping" template in the annex to help you conduct your own risk mapping exercise.

Developing a Risk Mitigation Plan and Addressing Risks

Key components of Risk Mitigation Plans

When you have mapped and categorized risks by their likelihood and impact, this should help you in crafting an effective response in the form of a Risk Mitigation Plan. As mentioned, risks falling into the High Likelihood/High Impact category should be prioritized for immediate action. Meanwhile Low Likelihood/High Impact risks typically require contingency planning or SOPs, while High Likelihood/Low Impact and Low Likelihood/Low Impact risks might need constant monitoring rather than immediate mitigation plans.

A Risk Mitigation Plan outlines the specific steps, tools, and strategies you will use to reduce or eliminate the identified risks. Remember, the goal is not usually to eliminate risks completely—this is often not possible—but to manage them and minimize their impact or likelihood.

In developing your Risk Mitigation Plan and when looking at specific risks you have prioritized, you can ask yourself questions such as:

- What immediate actions can I take to reduce the likelihood of the risk?
- If this risk does happen, how can I reduce its damage or consequences?
- Is this risk something that can be controlled, or is it external and beyond my influence?
- What external sources of support and resources do I have access to that could help me reduce its impact or likelihood?

By asking yourself these questions, you or your organization can start to develop a plan for addressing the most urgent and impactful risks. In addition to specific mitigation strategies (see “Immediate risk mitigation steps” for some examples), a detailed Risk Mitigation Plan would also outline aspects such as which resources will be allocated for each risk mitigation step (e.g. financial resources, time, technical tools and devices, and partners); who is responsible for the proposed risk mitigation step (e.g. yourself or someone else at your organization); what the timeline is for the risk mitigation step; and what the contingency plan is for risks that cannot be mitigated or for which the proposed risk mitigation steps prove to not be successful.

Please see the “Risk Mitigation Plan” template in the annex to help you put together your own Risk Mitigation Plan relevant to your situation.

Immediate risk mitigation steps

In the following sections, you can find some examples of immediate risk mitigation steps you can take to address common risks you or your organization might face. This list is by no means intended to be exhaustive and there are a multitude of other steps you might want to take, depending on the unique circumstances of the risk situation you find yourself in. Please also refer to the list of additional readings and other organizations providing support to at-risk individuals and organizations that you can find at the end of this document.

Psychosocial Safety

Strategies and tools to address common psychosocial safety risks include:

- **Self-awareness strategies:** Self-awareness involves being intentional about gaining knowledge of our own feelings, our own thoughts, our behaviors, our motivations, and how our body communicates with us. It provides us with information about how we are feeling and how we are responding by giving ourselves permission to look at ourselves introspectively and be vulnerable. One strategy we recommend would be the "hand exercise" for self-reflection. This simple exercise can be a helpful tool for increasing self-awareness and promoting emotional wellbeing. In this exercise, you use your hand as a visual aid to reflect on different aspects or emotions that are important to you. Each finger of your hand represents a different aspect or emotion, including your motivation(s), trust, happiness, hope, calmness, and what grounds you. Take a few minutes to go through each one of your fingers and the palm of your hand and reflect on each of the areas associated with it. Consider how each of these aspects might impact your work and overall wellbeing.

- **Stress management and grounding techniques:** Relaxation techniques, such as meditation, yoga, or anything else within your cultural setup can help you to feel more relaxed and reduce stress. Other effective strategies in managing stress include grounding and soothing. In some situations, when we are not able to manage on our own, it will be important to talk to someone. This can be a professional mental health provider or someone else from our support system, such as family or friends, who can help us address the challenge that is stressing us out. An example of a grounding technique would be to lie down on the ground or sit down comfortably in a chair and then, starting with the body, press your toes into the floor and squeeze tightly. The contact between your body and the ground and you pressing down helps the system feel more grounded. Finding a grounding object is another effective method. A grounding object can be anything (e.g. a stone, a piece of art that you feel in touch with) that you can touch. Grounding objects can help you feel calmer and more grounded when you're experiencing

anxiety or stress by redirecting your attention to the present moment and the object in front of you.

- **Investing in your psychosocial well-being and resilience:** Reinforcing the importance of proactive ownership of your psychosocial well-being can include many behaviors that have a positive impact on your psychosocial wellbeing, such as exercising, spending quality time with friends or family, meditating, engaging in creative work, going for a hike, or simply listening to music. A personal objectives plan can be a helpful tool in intentionally investing into your psychosocial well-being and resilience. This plan would include objectives that you can put in place to feel in control and able to change what can be changed, as well as able to transform, enhance, and overcome aspects that weigh you down. Emotional objectives, physical objectives, social objectives, intellectual objectives, spiritual objectives, environmental objectives, and professional objectives are all aspects of goals that you could work on and develop in order for you to feel resilient, to not feel stuck, and to feel that you are gaining control over your life.

Digital Safety

Strategies and tools to address common digital safety risks include:

- **Securing your passwords:** Creating strong passwords is crucial for protecting your online accounts from unauthorized access. To craft a robust password, start by incorporating a mix of uppercase and lowercase letters, numbers, and special characters. Avoid using easily guessable information like your name, birthdate, or even the names of your pets or relatives. Instead, opt for a random combination of characters that are impersonal and unrelated to your personal details. Additionally, consider using a passphrase—a memorable combination of words or a sentence—that is easy for you to remember but difficult for others to guess. Regularly update your passwords (every six months or so) and refrain from using the same password across multiple accounts to further safeguard your online presence. Do not re-use passwords or share accounts. You can use a password manager like KeepassXC or Bitwarden to keep your information stored safely. Using a password manager means that you don't have to remember all your different passwords – the manager remembers them for you.

- **Managing your online footprint:** While social media can be an important information source, sharing too much information online can have some serious downsides. Almost any commercial product online that you do not pay for (such as social media and email) is not actually "free;" you pay for it with your data. As everything you do on the internet will stay there forever, you can take some precautionary steps to not give away too much of your information

in the first place. This can include steps such as not posting too much personal information or information about your organization online (e.g. birthdays or your relatives' names), regularly checking privacy and security configurations on your accounts, as well as using two-factor authentication (2FA).

- **Securing your data and communication:** To protect your data, start by making a list of sensitive information and documents that you need to take extra care of. Make sure you have a clear plan for how best to protect each document. It is important to keep all this sensitive information secure in case of loss or theft of your storage devices or computers so you can avoid unknown people accessing your data. Your ability to protect your communication is, to a large extent, determined by our choice of the means of online communication. One tool for secure communication is Signal, which protects not only you but also the people you communicate with. Signal's software is free and open-source[1]. Also consider using a Virtual Private Network or VPN[2] like Tunnelbear while you navigate the web, as well as a secure mail provider like Protonmail, which is a no-cost alternative and can be used everywhere you go because it is web browser-based. Remember to never send sensitive data over free commercial email accounts like Gmail, Yahoo, or Hotmail.

Physical Safety

Strategies and tools to address common physical safety risks include:

- **Conducting Risk Assessments:** To understand and be able to better assess the different challenges you may face as a media professional, social communicator, media outlet, or CSO, risk assessments are essential. Refer to earlier sections in this document for a detailed description of how to map, assess, and mitigate risks.

- **Practicing situational awareness:** The goal of practicing situational awareness is to develop the skills and mindset necessary to become more attuned to the subtle and overt dynamics of your environment. Situational awareness involves paying close attention to your surroundings and remaining alert to any potential risks or threats. One powerful tool for improving your ability to assess and respond to your environment is the Observe, Orient, Decide, Act (OODA) loop. The process involves four key steps: Observe your environment to gather information; Orient yourself by analyzing what you observed and understanding its relevance; Decide on the best course of action, and Act by implementing your decision. By continuously cycling through

[1] Open-source refers to something—usually software—that is made freely available for anyone to use, modify, and share. Its source code is openly shared, allowing developers to collaborate, improve it, and adapt it to their needs. Open-source software is often considered safer because its transparency allows many people to review, identify, and fix vulnerabilities, creating a more secure and reliable product through community-driven development.

[2] A VPN, or Virtual Private Network, is a tool that helps protect your privacy online. It creates a secure, encrypted connection between your device and the internet, hiding your IP address and making your online activity harder to track. VPNs are often used to protect sensitive information, access content restricted in certain locations, and stay safe on public Wi-Fi networks.

these four steps, you or your organization can stay alert, rapidly adapt to changing situations, and mitigate potential risks and threats.

- **Planning:** Thorough and risk-sensitive planning is directly linked to risk assessments and situational awareness and is imperative for conducting tasks in a safe and secure manner. There are typically five key planning steps, namely self-awareness and identity management, situational awareness, risk assessment, safe communication, and preparing a grab bag with essentials. Self-awareness and identity management include assessing your unique vulnerabilities, and looking at your personal and organizational profile that might make you a target. Situational awareness, as described, involves staying informed about your surrounding environment. The risk assessment includes identifying and prioritizing the likelihood and impact of risks. Ensuring safe communication involves secure tools and practices to protect sensitive information, and preparing a grab bag includes putting together a bag with essential items for emergency situations to ensure readiness in case of sudden danger.

Additional Readings

Find below a curated list of resources that delve deeper into some of the key topics introduced throughout this resource kit. These materials provide further insights to help you better understand concepts such as risks, risk mapping, and risk mitigation planning, as well as provide additional guidance on some key tools and strategies to mitigate risks you or your organizations might face.

Risk mapping and risk mitigation planning

- On *risk mitigation planning*: Committee to Protect Journalists (CPJ). (n.d.). Assessing and Responding to Risk. Committee to Protect Journalists. Retrieved February 9, 2024, from https://cpj.org/reports/2012/04/assessing-and-responding-to-risk/#:~:text=Always%20prepare%20a%20security%20assessment

- *On safety planning (Module 1):* Journalism Courses Knight Center. How to Report Safely: Strategies for Women Journalists & Their Allies - Journalism Courses Knight Center. Retrieved November 21, 2024, from https://journalismcourses.org/product/how-to-report-safely-strategies-for-women-journalists-their-allies-2/

Risk mitigation strategies

Psychosocial safety

- On *online harassment*: PEN America. (n.d.). Online Harassment Field Manual - PEN America. Online Harassment Field Manual. https://onlineharassmentfieldmanual.pen.org/
- *On general self-care tips:* Miller, N. (2021, July 1). Self-care tips for journalists -- plus a list of several resources. The Journalist's Resource. https://journalistsresource.org/home/self-care-tips-for-journalists-plus-a-list-of-several-resources/
- Journalism is Stressful Work. Here Are Resources for Reporters Coping with Trauma. (2025). Retrieved October 2, 2025, from Gijn.org website: https://gijn.org/resource/journalism-is-stressful-work-here-are-resources-for-reporters-coping-with-trauma/
- *On how to deal with trauma:* Cobham, K. (2019, May 29). How journalists can take care of themselves while covering trauma - Poynter. Poynter. https://www.poynter.org/reporting-editing/2019/how-journalists-can-take-care-of-themselves-while-covering-trauma/

- *On how to report on trauma:* Karki, A. (2018, October 30). 6 tips for protecting your mental health when reporting on trauma. International Journalists' Network. https://ijnet.org/en/story/6-tips-protecting-your-mental-health-when-reporting-trauma

Digital Safety

- On *secure passwords*: Bitwarden's World Password Day Global Survey Full Report
- On *secure passwords*: Nordpass's Most Common Password List
- On *secure passwords* (self-paced course):Totem Project. Secure Passwords. Learn.totem-Project.org. https://learn.totem-project.org/courses/course-v1:Totem+TP_SP_001+course/about
- On *2-Factor Authentication* (Youtube Video): CSP. (2021, September 28). Two Factor Identification. YouTube. https://www.youtube.com/watch?v=h1YtBDNHzXU
- On *secure messaging apps*: NordVPN. (2024). What is the best secure messaging app? NordVPN. https://nordvpn.com/es/blog/most-secure-messaging-app/
- On *secure software and apps*: PrivacyTools - Encryption Against Global Mass Surveillance. (n.d.). PrivacyTools. https://www.privacytools.io/
- *On how to protect your sources:* Hauk, C. (2020). Pixel Privacy Logo. Pixelprivacy.com. https://pixelprivacy.com/resources/journalist-privacy-guide/
-

Physical safety

- On the *OODA Loop*: MindTools | Home. (n.d.). Www.mindtools.com. https://www.mindtools.com/a3ldgz1/ooda-loops
- On *Cooper's Colors codes*: Simoes, P. F. (2023, March 7). What's Your Safety Colour? My Krav Life. https://medium.com/my-krav-life/whats-your-safety-colour-65f10fa41bfc
- *On how to cover unrest:* Tompkins, A. (2021, January 15). 25 guidelines for journalists to safely cover unrest. Poynter. https://www.poynter.org/reporting-editing/2021/25-guidelines-for-journalists-to-safely-cover-unrest/
- *On risk assessments and planning:* PEN America. (2024, July). Risk Assessment and Physical Safety: What Every Journalist Should Know - PEN America. https://pen.org/risk-assessment-and-physical-safety-what-every-journalist-should-know/
- *On covering elections:* IWMF. (2024, August 12). From protests to the polls, protecting your physical safety in the field. https://americanpressinstitute.org/protecting-your-physical-safety-in-the-field/

Risk Mapping Template

assess and categorize them depending on their likelihood and impact. This tool can help you or your organization visualize threats and organize them by priority to then, as the next step, use the risk mitigation template to plan how you will respond to them.

Step 1: List all potential risks: As part of this step, you would brainstorm about all potential risks you can think of. Remember to look at risks holistically, including all things that might affect your physical, digital, and psychosocial wellbeing. For now, there is no need to categorize or rank the risks, but just to note down everything you can think of that might affect your own or your organization's safety.

Step 2: Rank all potential risks: As part of this step, assess and categorize all risks you listed under Step 1, using the concept of the Likelihood/Impact graph. Add additional rows as needed.

Risk	**Likelihood** (Low/Medium/High)	**Impact** (Low/Medium/High)

Risk Mitigation Plan Template

The below Risk Mitigation Plan template builds on the Risk Mapping template above. Now that you have mapped and categorized risks, use this table to plan your response to the risks you have identified. Remember to prioritize risks that fall into the High Likelihood/High Impact category. Add additional rows as needed.

Risk	**Priority** (Low/Medium/High)	**Mitigation Steps**	**Responsible Party**	**Deadline**	**Contingency Plan**