SIPRI's Risk Management Policy 2025

Approved by Director
May 2025

Introduction

SIPRI's institutional risk management model identifies and analyses risks that can affect the overall business and extraordinary risks with the potential for major consequences.

These risks are summarized in a risk register. The risk register also indicates which measures are in place, are under development or need to be addressed to mitigate the risks or to minimize the negative impact on SIPRI's ability to fulfil its mission and achieve its objectives.

Method

The organization undertakes risk assessments annually, or on an ad hoc basis when significant changes or emerging risks are identified. The risk levels are assessed and graded 1 – 5 for probability of the event and 1 – 5 for the severity of the impact if the event occurs. The overall assessed risk is the probability multiplied by the consequence. Following a common practice, risks that have a combined grade of 9 or below are regarded as tolerable and left to one side. They are, however, revisited in the next assessment round. Mitigation measures are specified for each risk of more than 9. The risk is then regraded in the same way as before to identify the level of residual risk.

Consequence

Probability

	1 Negligible	2 Minor	3 Moderate	4 Significant	5 Severe
5 Very likely	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Very unlikely	1	2	3	4	5

1 – 4: low, 5 – 14: Medium, 15 – 25: High

Definitions
Risk: the "effect of uncertainty on objectives" (ISO 31000 Risk Management)

Risk management: the process of identifying, assessing and controlling financial, legal, strategic and security risks

Responses to risk
There are several possible response strategies to risks. SIPRI applies one of the following approaches to each identified and prioritized risk:

Risk avoidance
Avoidance is a method for mitigating risk by not participating in activities that may negatively affect the organization. Not making an investment or starting a project are examples of such activities as they avoid the risk of loss.

Risk reduction
This method of risk management attempts to minimize the loss, rather than completely eliminate it. While accepting the risk, it stays focused on keeping the loss contained and preventing it from spreading. An example of this in health insurance is preventative care.

Risk sharing
When risks are shared, the possibility of loss is transferred from the individual to the group. A corporation/consortium is a good example of risk sharing — a number of investors pool their input and each only bears a portion of the risk that something may fail.

Transferring risk
Contractually transferring a risk to a third-party, such as, insurance to cover possible property damage or injury shifts the risks associated with the property from the owner to the insurance company.

Risk acceptance and retention
After all measures have been implemented, some risk will remain since it is virtually impossible to eliminate all risk (except through risk avoidance). This is called residual risk.

Risk Register
SIPRI's organizational risk register is confirmed by the Senior Management Team and presented to the Governing Board for discussion. The risk register is reviewed at a minimum on an annual basis, and additionally on an ad hoc basis in response to particularly challenging circumstances.

Separate risk registers are also available when required for separate research projects. These project risks registers are not included in the overall register.