Safety and risk management policy at CMI

Contents

1 Introduction

1.1 The Safety and Risk Management Policy forms part of the Institute’s governance and quality arrangements.

1.2 Safety (or Risk) management is not an isolated activity but is one element, together with planning, project and performance management, of effective governance and management. The focus is on those risks that could disrupt achievement of the Institute’s strategy, directly through operational downtime or reputational issues or more indirectly through harm on equipment, staff or the general working-environment. Risk can be translated in many different ways, and there is both negative and positive risk in order to achieve the Institute’s strategy.

1.3 The purpose of this policy and the supporting guidance is to establish a framework for the Institute’s approach to safety or risk management by clarifying the roles and responsibilities of the CMI-director, other parts of the management, the operational staff responsible for IT, travel and HR and different projects and programs, and the rest of the staff. Another purpose is to establish a system for continuous awareness and learning, and systematic reviews. A third purpose is to secure that we are in line with requirements given to us through regulations and law, ie Arbeidsmiljøloven, Internkontrollforskriften and Data Protection. In addition, many funders specify their own requirements, and risk management is one factor in their assessment of funding decisions.

2 Definitions

Safety is defined as: *A state where a few things as possible go wrong*

Risk is in NS5814 defined as: *The correlation between likelihood and consequence of an unwanted incident.*

Another definition (Safety 2): *The system’s ability to succeed under varying conditions*

Safety and risk management: *The planned and systematic approach to anticipating, identifying, evaluating and mitigating risk but also to facilitate everyday work, to anticipate developments and events, and to maintain the adaptive capacity to respond effectively to the inevitable surprises (inspired by Hollnagel et al)*

3 Principles

- The risks are identified through risk assessment.

- New threats are to be picked up and evaluated continuously.
- Safety measures (barriers) to prevent accidents/incidents shall at all times be proportionate to the acceptable level of risk
- Crisis-management-plans shall exist in areas where the consequences of an incident are perceived to be large.
- When incidents occur, barriers shall help limit the damage and help us quickly to return to normal operation.
- Safety shall be an integrated part of the work of the organization.
- A sound and good safety culture shall be stimulated.
- Ownership to risk areas shall be assigned in order to secure consistent and regular focus, but at the same time, staff should be encouraged to give their concerns to the "risk-owner".
- All employees shall receive the necessary training to fulfill their security responsibilities.
- The 'owner' of the risk should have in place early warning mechanisms to alert the Institute so that remedial action can be taken to manage any potential hazards.
- Employees shall be perceived as a resource in our safety work
- Legal compliance is a minimum standard.

4 Policy statements major risk areas

4 major risk areas have been identified;

The first is overseas travel. Much of our work takes place overseas in locations that are inherently risky. We are responsible for the well-being of our staff. We therefore seek to ensure that work with partners overseas and in particular, overseas travel for our own staff is informed by robust risk assessments, and that travelling staff are trained for and supported during their individual journeys. CMI will not require staff to travel where the risks are assessed to be excessive.

A separate crisis management plan has been made to handle incidents efficiently. A separate policy on travel security sets out the Institute's approach to assessing risks at the point of project proposal preparations and planning of individual travels. This reflects our duty and practice in caring for and supporting travelers.

The second risk that stands out is operating risks connected to ICT: We are dependent on our

ICT-equipment in almost all we do, and increasingly so during a pandemic like Covid-19. The risk for operational downtime has increased as servers and software are increasingly interlinked, not least through the internet. The goal of our safety management in this area is to protect the values CMI manages through our ability to solve priority tasks and services and secure the integrity and confidentiality of CMI's information against illegal acts and accidents. The third risk is inability to retain staff (turnover of staff). The risk has increased as a large proportion of newcomers are hired from abroad, and due to younger staff having different demands from employers. In 2020 have been implemented through recruitment of an HR-adviser who immediately focused on improving CMI onboarding and offboarding processes to secure better expectations-management and better integration of newcomers. Specifically, CMI now offers an information pamphlet to help navigate the transition to Norway for employees who move to Bergen from abroad, and all new employees are invited to an introduction day. In relation to offboarding, CMI will also systematically implement formal exit-interview.

The fourth risk is related to data protection, and especially potential failure to do risk assessments and implement risk reducing measures when collection personal data. CMI has also identified weaknesses and the lack of routines for deletion of data when not needed anymore. CMI has from 2019 hired a dedicated resource in 20 % to go through all routines and support researchers in the needed assessments when doing research in need for the collection of personal data

Risks have also, through the organizational survey, been identified in other operational areas such as fire, burglary and theft and possible treats and attacks on CMI staff presenting/writing potential controversial reports. Work related stress, primarily connected to too much to do, or not sufficient project earnings have been identified as a health risk. On the other side,a positive psychosocial working environment will reduce risks. All areas are part of systematic risk assessments and regular reviews of the routines set up to reduce the probability or consequence of an incident.

5 Roles and responsibilities

The Director approves CMI's safety policy and assesses the goals for CMI's safety level. The Director is responsible for overseeing the safety management and the policy implementation. The overall responsibility cannot be delegated but the executive follow up work can be delegated to the Admin and Finance director. The responsible for ICT, HR and HES are responsible for preparing and updating CMI's policy documents, regularity of risk assessments, and for awareness raising activities at CMI. The responsibility for CMI's travel policy and for awareness raising activities in that area is delegated to HR in close cooperation with CMI travel coordinator. All senior staff are responsible for encouraging good risk management practice within their areas of responsibility, and all project managers (researchers and professionals) will need to take into regard the risk for the projects that they lead or support.

6 Periodic reviews

The Director will regularly review CMI's Safety and Risk Management Policy and the development of risk levels through systematic risk assessments.

The director will, together with the Admin and Finance director and the Deputy Director review the effectiveness of the internal control system. As part of this, this body will consider:

i. the management's approach to risk;
ii. the appropriateness of the level of delegation of authority;
iii. prioritization of risks;
iv. timely identification and assessment of risks;
v. the Institute's ability to learn from its problems and apply this in its learning.

The responsible for the risk assessments shall present these and a draft action plan on a yearly basis (autumn) to the management.

The management group shall every autumn discuss the safety and risk management action plan.

7 Key elements of the CMI Safety and Risk Management Policy

Assessing risks

Effective risk management requires risks to be anticipated, identified and assessed regularly, and actions must be taken to manage the risks.

Most relevant authorities on risk management advocate two main parameters for assessing risks. The parameters are:

- likelihood, ie how likely is it to happen
- impact, ie how significant might the consequences be

Risks which are 'very high' on either scale require active monitoring.

Consequence/Impact:

Very low — no significant disruption; adverse publicity unlikely; litigation unlikely; financial loss modest; funder/partner relations unaffected

Low — short term disruption; careful PR required; litigation unlikely; moderate financial loss; funder/partner relations unaffected

Moderate — short term disruption; reputational damage; litigation possible; significant financial loss; funder/partner relations may be affected

High — medium term disruption; adverse publicity; probable litigation and difficult to defend; significant financial loss; funder/partner relations affected

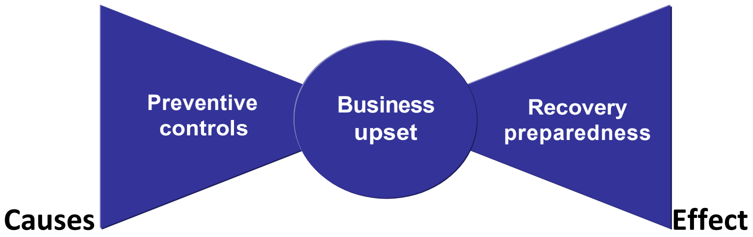
Very high — sustained disruption; significant reputational damage; litigation highly likely and costly; significant financial loss; funder/partner relations seriously affected

Likelihood:

Very low	every 50-year or more rare
Low	one every 10 years
Moderate	one every 5 years
High	every year
Very high	more than once a year (as likely as not)

Impact	🟨	🟨	🟨	🟥	🟥
	🟩	🟨	🟨	🟥	🟥
	🟩	🟨	🟨	🟨	🟨
	🟩	🟩	🟨	🟨	🟨
	🟩	🟩	🟩	🟨	🟨
	Likelihood				

The perspective of why things normally go well has to be included in the assessment.



An bow-tie method shall be applied on risks perceived to be moderate or high in order to to identify possible proactive barriers to reduce or avoid incidents, or to reduce the consequences if the incident happen.

Details of the Institute's approach to assessing risks will be developed and will be found in annex B to this policy document

Monitoring and learning

Some risks will be put on a Strategic Risk List, especially those with a 'High' or 'Very high' risk score. Clusters/units and departments will be asked to review the operational risks captured in their Registers termly. The Director and the management group, which meets regularly, keep the Strategic Risk List under review.

We will learn from our experience of risk management and seek to share issues and ideas with staff to enable them to work effectively in a risk-based manner.