



Institutional policy

Organisation of risk management

**Risk management
and Internal Auditing Unit
Federal Secretariat**

November 2017

IP | 08





Institutional policy

Organisation of risk management

1. RISK MANAGEMENT: PURPOSE AND APPROACH	3
2. SCOPE	3
3. PRINCIPLES AND PROCESSES	3
3.1 The principles	
3.2 The process	
4. ROLES AND RESPONSIBILITIES	4

1.

Risk management: Purpose and approach

- Identifying and assessing risks using a prospective approach that anticipates the future;
- Defining strategies and putting in place actions in order to stabilise risks or bring them down to an acceptable level;
- Monitoring and overseeing the risk management and control system from operational management to internal control and auditing.

To achieve the above, HI has put in place a risk management system which:

- Supports decision-making processes in line with the organisation's vision, mission and strategy;
- Ensures an integrated approach to risk management;
- Formalises and operationalises its engagement in this activity;
- Coordinates internal planning, continuous improvement and internal control processes.

2.

Scope

- HI's risk management policy and measures apply to all the entities in the HI network (Federation, national associations, headquarters and field programmes);
- Risk management concerns all the dimensions of the organisation: Governance, steering, operations, purchasing and resource management, communications and external relations;
- Specific internal bodies are tasked with promoting, coordinating and evaluating HI's risk management policy. However, risk prevention and managing their potential consequences concerns all the organisation's members and staff.

3.

Principles and processes

Risk management is an integral part of our organisational strategy and operational planning, alongside our approach to quality and accountability. Our risk management approach is based on principles and processes.

3.1

The principles

HI's risk management:

- Is consistent with the organisation's vision, mission and strategy;
- Applies to all our organisational systems, processes and activities;
- Is based on a system of regular consultation and information-sharing;
- Takes into account the organisation's internal context and external environment;
- Supports decision-making processes;
- Interacts with our existing systems of internal control, monitoring & evaluation, auditing and insurance;
- Supports our continuous improvement processes.

3.2

The process

The process is made up of the following stages:

- **Identification** – Identifying negative events which could, over a given period of time, prevent or delay the achievement of the organisation's strategic objectives, affect its operations or threaten its existence¹.
- **Analysis** – Evaluating situations, causes and risk factors, the probability of occurrence and potential impact of the materialisation of a risk.

1. Definition of risk: "Possibility of an event occurring that will have a negative impact on the achievement of the organisation's objectives". Risks are measured in terms of impact and probability over a given period of time.

- **Management** – Defining and implementing existing or additional measures necessary for preventing risks (acting on probability) or mitigating them (reducing the negative impact if the risk were to materialise).
- **Monitoring** – Conducting ongoing monitoring and assessment of risks and related prevention and mitigation measures in order

to maintain the efficiency and relevance of risk management.

- **Reporting** – Keeping the key executive and governance bodies regularly informed to ensure they have the necessary understanding and knowledge of the risks and can adapt their steering and management accordingly.



Zoom 1 : Risk mapping

After identifying the risks, the next step involves establishing a declarative rating of their impact and probability, placing them on a simple rating scale and creating a **hierarchical graphical representation**.

Quantification of impact: To estimate the seriousness of the consequences if the risk were to materialise. To measure this, it is best to use a financial value as this will make it easier to establish comparisons and, in the long run, evaluate the global cost of risks for the organisation's resources and the non-institutional funds on which its sustainability depends.

Quantification of probability: To evaluate the possibility (% of chances) of the risk materialising over a given period (in HI's case, the three-year sequences of our multi-annual strategy).

The evaluation of probability is based on the organisation's current situation and current prevention, protection and risk-handling

measures. This evaluation must also take into account the nature, frequency or number of certain materialised risks over a given period.

Action plans: On the basis of this risk mapping, the managers in charge of risk monitoring draw up action plans. According to the strategic choices made, which can range from risk avoidance to assumed management of risk or sharing this responsibility with a third party, these actions plans should enable:

- **Prevention measures to be upgraded** to influence the probability or reduce the percentage chance of risks materialising;
- **Protection measures to be upgraded** to reduce the impact of any consequences and therefore the seriousness of the event;
- And they should orient the **control measures**, the focuses of internal audits and the search for suitable insurance coverage.

4.

Roles and responsibilities

- **The Audit Committee of the federal Board of Trustees'** is tasked with verifying the organisation's risk management practices on behalf of the Board.
- **The Risk Management Committee (CMR), attached to the federal Directorate** and reporting to the Managing Director, is responsible for the rollout, implementation, evaluation and improvement of our risk management policy and measures (see

extract from the attached Terms of Reference). Consequently, the CMR is the executive body that approves the risk mapping. It forwards the key information resulting from its workings to the Board of Trustees' Audit Committee. The CMR also carries out a periodic revision of risk management policy.

- The CMR works in conjunction with **Risk Management and Internal Auditing Unit** which coordinates the development of the risk map and the implementation of the annual internal audit plan.
- **The federal and national directors** of HI's network take part in developing the

global risk map. Within the scope of their individual responsibilities, they support the implementation of risk management policy in all areas.

- The **directors** therefore take part in identifying, analysing, managing, monitoring, evaluating and providing feedback on significant risks in their sectors of responsibility and in their own associations, divisions and services. They promote a positive risk management culture among their staff members. To do so, they draw on a network of federal functional advisers who analyse the information emanating from activity managers and heads of federal services, national associations and field missions.
- **Managers and heads of services** ensure that all their staff understand and assume

their roles. They encourage access by their staff to information and training initiatives on the subject. They contact resource staff and the relevant services to help their teams on matters relating to risk management. They forward information on risks to their directors and to the functional advisers.

- Furthermore, as they are responsible for the internal controls of the processes and activities they are in charge of, they are the best placed to periodically reassess the risks and control measures.
- All the organisation's **members and staff** have a role to play in risk management. They must keep up-to-date with and support initiatives concerning the implementation of the risk management measures recommended by management.



Zoom 2: Lines of defence against risk at HI

General framework

By delegation of authority from HI's governance bodies, the executive management bodies set the policy framework and the rules to be applied by everyone.

1st line of control:

Internal control is a managerial responsibility. Line-managers delegate tasks, but must also check that directives and rules are being correctly applied (random sampling without having to check everything).

2nd line of control

The second line is made up of specialised divisions and services which guide the implementation of policies, technical standards and rules. These services also

carry out monitoring by means of indicators, as well as evaluations and controls in their areas of competence and expertise. Insurance is also taken out to protect the organisation against the consequences of risks relating to persons or assets and civil liability.

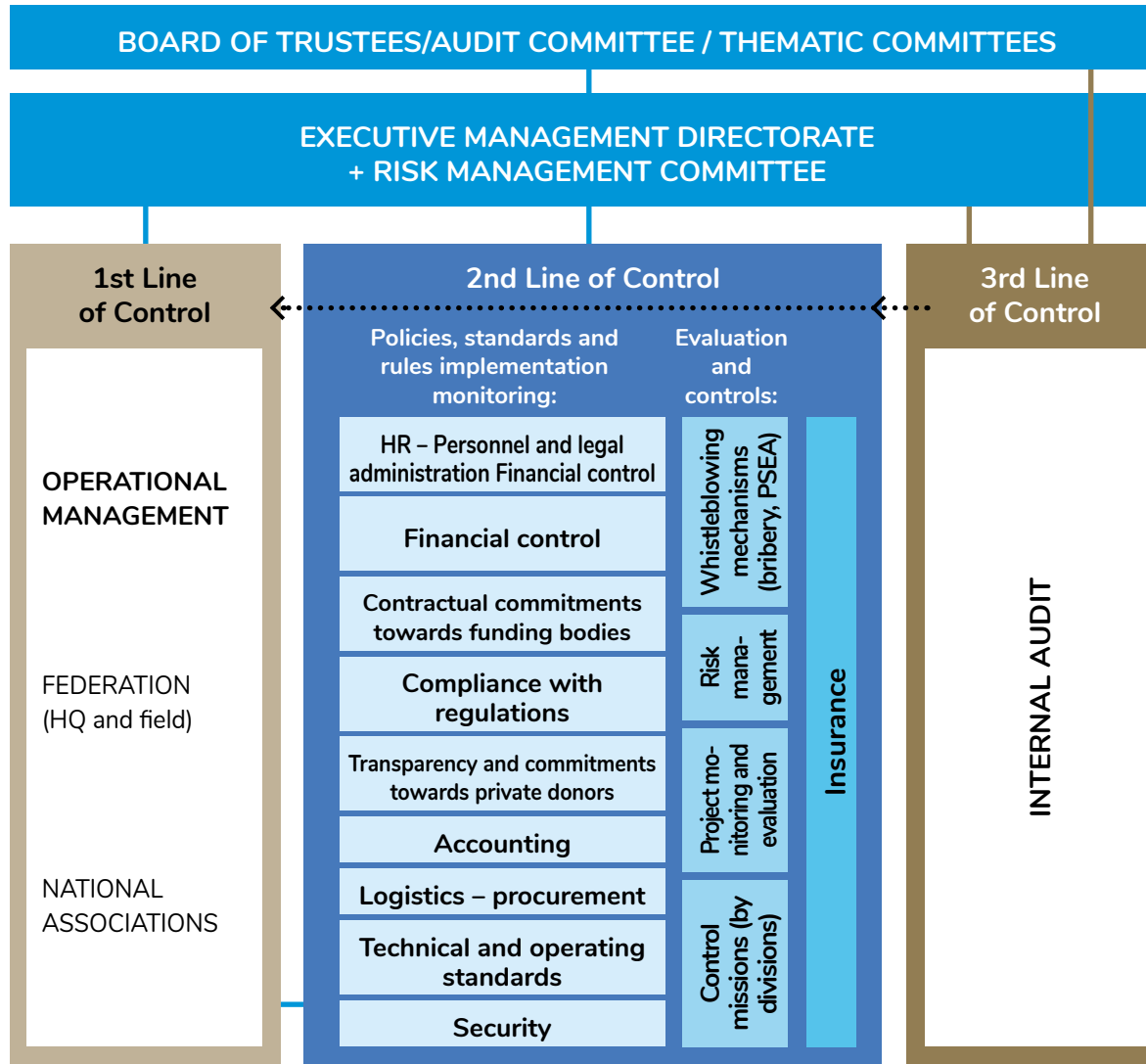
3rd line of control

Internal audits are the third line of control. The findings of audits inform the Directorate and Board of Trustees about the level of risk control in the services, programmes and entities audited and enable adjustments to be made to prevention and management systems.

→ See attached diagram

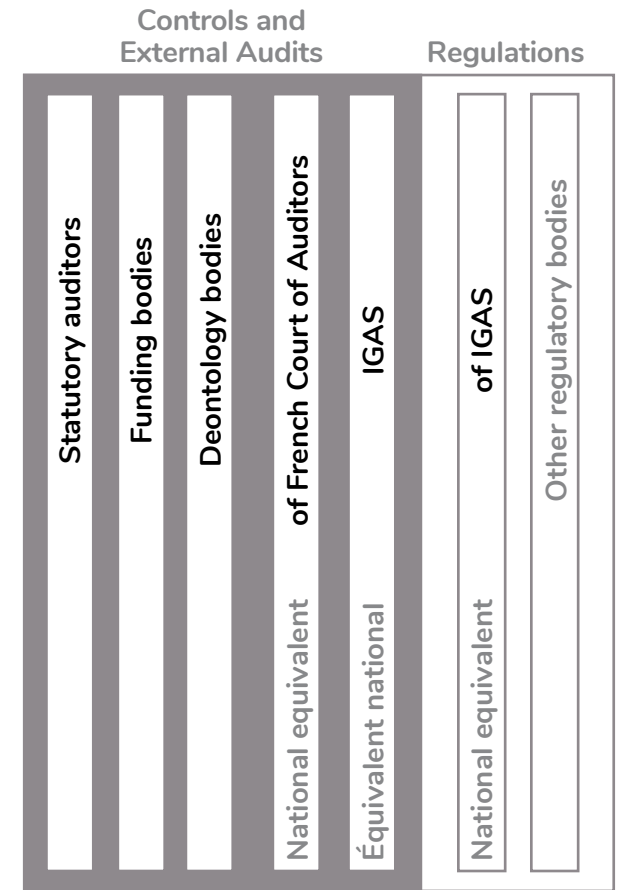
HI Risk Control and External Environment

HI Risk Control Actors



Institutional actors who exert official or unofficial control on the organization, how it is operated, or its activities

Surveys
Mass media & Social Networks



Policy approved by the federal Directorate in February 2017

Contact:

Risk management and Internal Auditing Unit
Federal Secretariat
138 avenue des Frères Lumière
69008 Lyon – France
l.loiacono@hi.org

Internal document

Access authorised for partner organisations



Organisation of risk management

This document presents the scope, principles and processes of risk management at Humanity & Inclusion (HI). It also explains how risk management is organised, which internal bodies are directly involved and how roles and responsibilities are distributed.

Humanity & Inclusion
138, avenue des Frères Lumière
CS 88379
69371 Lyon Cedex 08

publications@hi.org

