GSIF POLICIES, STANDARDS AND PROCEDURES

Risk Awareness

GOOD SHEPHERD INTERNATIONAL FOUNDATION ONLUS

"What is the duty of a shepherd...to strengthen what is weak, to bind up what is broken, to bring back what was driven away...to preserve what is well and strong."

St. John Eudes

Index

1. Introduction
2. Risk Perimeters
3. Risk Tolerance
4. Risk Ownership
5. Risk Management Process
6. Risk Management Flowchart
7. Risk Management Tools
8. Risk Awareness Timeframe
9. Some risks of Risk Management
10. References

Glossary

GSIF
Good Shepherd International Foundation

MDO
Mission Development Office

OLGCS
Sisters of Our Lady of Charity of the Good Shepherd

NGO
Non-Governmental Organization

PM
Program/Project Manager

F&A
Finance and Administration

M&E
Monitoring and Evaluation

ISO
International Organization for Standardization

Near miss
is an unplanned event that did not result in injury or damage - but had the potential to do so.

Risk awareness
the raising of understanding within an organization of what risks exist, their potential impacts, and how they can be managed.

Risk management
the process of identifying, prioritizing and responding to risks across an organization. Risk management includes activities to realize opportunities while mitigating threats.

Risk
the effect of uncertainty on objectives (ISO 31000[1])

Impact
the consequence of a risk event materializing.

Probability
the likelihood that a risk will occur.

Risk appetite/tolerance
the amount of risk GSIF is willing to take on in pursuit of its mission and objectives. It varies for different types of risk.

Risk response
includes the decisions made to respond to a risk by either tolerating it, treating it (mitigating, transferring, or terminating), or exploiting it.

Risk Register
a repository or risk log of identified risks, which includes priority ratings, and risk response strategy.

Risk Assessment
the overall process of risk identification, risk analysis, and risk evaluation.

Risk Matrix
a tool for ranking and displaying risks by identifying ranges for consequences and likelihood.

Risk Owner
the person or the organizational body responsible for managing risks related to the objective he/she/it is accountable for. It means monitoring risks, proposing risk response and ensuring necessary actions are taken. That doesn't mean that the owner of a risk has authority over every decision or action that may change the level of the risk.

Risk Focal Point
the person responsible for gathering all the risk assessments at the different level of the organization and prepare the report to the Board of Directors. He/She does not have a managing role for Risk Management.

Uncertainty
refers to situations involving imperfect or unknown information.

1 - https://www.iso.org/news/ref2263.html

Having a robust Risk Awareness Culture helps to

- **Protect the mission and the people** involved in the pursuit of the mission;
- **Reduce the likelihood** of costly surprises;
- Prepare for **challenging events** and improve overall **resilience**;
- Improve the **quality of decision-making** at all levels;
- Improve **planning processes**;
- **Prioritize** limited resources;
- Increase **performance**;
- Improve stakeholders' **confidence** in the organization.

1. Introduction

According to the **ISO** (International Organization for Standardization) a Risk is defined as t**he effect of uncertainty on objectives.**

Risk does not necessarily mean something negative, a potential harm or a threat. A risk can also benefit GSIF and its Mission. To succeed in the pursuit of the Mission GSIF needs to take the right risks among all those available to it.

Risk awareness does not mean risk adversity. It means risk consciousness and willingness to manage uncertainties.

Although Risk Awareness can be seen as one of the new fashion approaches that characterize the societies from time to time, it is something that happens worldwide, across the different cultures over the centuries. On an individual level, it is a biological and psychological mechanism based on the need of self-protection and protection of other persons who we care for. The parents manage risks for the wealth of their children, the individuals manage risks for protecting themselves from harm or for taking advantage of certain situations. The shepherd manages risks for protecting its sheep. At the organizational level, it is a more complex mechanism that requires a strong will from top management and a clear methodology.

> Risk is the effect of uncertainties on objectives

⚠ Risk Areas

Sources of risks can be either **external or internal**, and may refer to one or more of the following areas.

- **SAFETY AND SECURITY** (accident, illness, violence, crime)
- **FIDUCIARY** (inadequate financial controls against corruption/fraud/ theft/diversion)
- **LEGAL/COMPLIANCE** (violating laws or regulations of international or governments issues)
- **OPERATIONAL** (inability to achieve objectives, capacity/ competence gaps, financial/ funding constraints, access constraints)
- **REPUTATIONAL** (damage to image and reputation)
- **INFORMATION TECHNOLOGY** (data breach/loss digital risk)
- **ETHICAL** (risk of harm caused by unethical behaviors including sexual misconduct/exploitation, inadequate duty of care or insufficient consideration of humanitarian principles)
- **POLITICAL/STRATEGIC/ GOVERNANCE**

Some risks are **insurable**, others are not and need to be managed by mitigating measures.

We also need to take into account that **some risks are objectives**, whereas some others **depend on the context and on the different perceptions and sensitiveness.** Sufficient diversity of perspectives, values and beliefs is important to ensure that different perspectives are taken into account and that the status quo is consistently and rigorously challenged.

Since being aware of risks is intended to help an organization achieve its objectives, risk awareness and management **must be integral to all aspects of the organization** including strategic planning, decision-making, operations and resources management.

Risk Areas

The list below is not intended to be exhaustive. There could be a different classifications of risk areas depending on the contexts and type of activities. The listed sources of risks can be either external or internal.

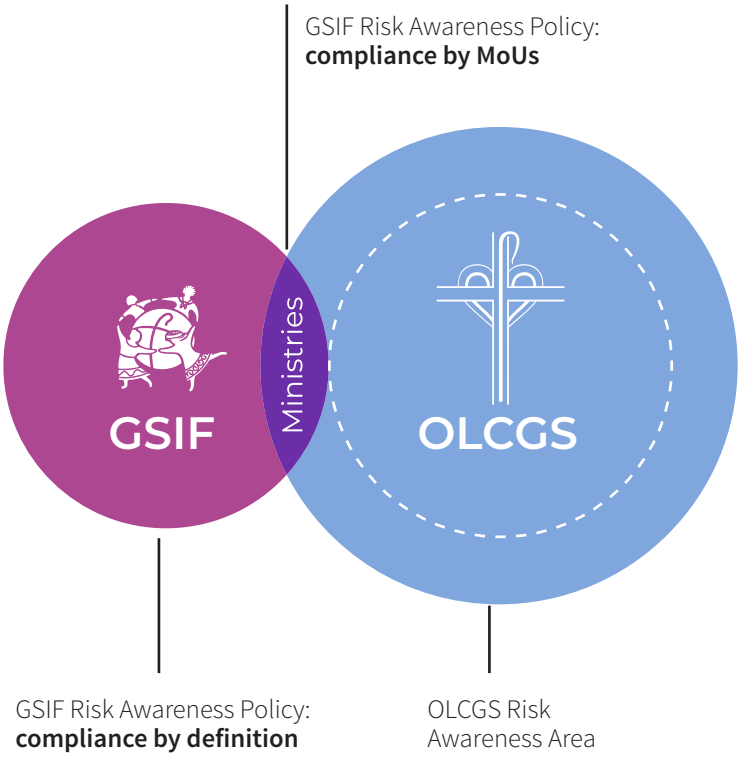
AREA OF UNCERTAINTY	TYPE OF RISKS	EXAMPLES OF CONCERNS OR OPPORTUNITIES (can be either negative or positive)
Safety and security	Accident, illness, violence, crime	• Failure of staff to follow Safety and Security procedures can result in potential injury and health and safety accident. • A realistic and careful evaluation of Covid-19 travel restrictions can avoid travel cancellations costs, operational and logistic complications.
Fiduciary	Inadequate financial controls against corruption/ fraud/theft/ diversion	• Failure of financial controls mechanisms resulting in (voluntary or involuntary) double funding on grants. • Having higher standards of accountability, segregation of duties, balance of powers can help to maintain a high degree of trust from stakeholders.
Legal/ compliance	Violating laws or regulations of international or governments issues	• Irregular modes of employment or mis respect of local labor laws can result in financial compensation claims, fine or litigation and/or reputational risks. • Understanding the legal frameworks, having specialized consultants, can help the organization avoid mistakes and seize opportunities.
Operational	Inability to achieve objectives, capacity/ competence gaps, financial/funding constraints, access constraints	• Failure of a robust needs assessment and strategic planning can result in ineffective actions and loss of credibility. • A lean structure, together with a strategic vision and a bit of resourcefulness, has allowed GSIF to respond promptly and effectively to the effects of the Covid-19 outbreak.
Reputational	Damage to image and reputation	• Failure of being risk-aware with regard to specific issues (such as child safeguarding, women empowerment, labor issues, etc.) can result in adverse media attention and loss of reputation with severe consequences on long-term sustainability of the mission. • Having higher visibility on specific issue can help to broaden the overall visibility of the organization.
Information technology	Data breach/loss digital risk/IT inadequacy for remote working	• Loss of digital records through inadequate IT systems can result in fine or litigation and/or reputational risks. • Using non-secure email accounts can result in IT fraud and sound financial loss. • A cutting-edge IT infrastructure, together with an open and flexible staff and an organization of work by objectives, can help to do smart working in a productive and effective way.
Ethical	Risk of harm caused by unethical behaviors including sexual misconduct/exploitation, inadequate duty of care or insufficient consideration of humanitarian principles	• Failure to promote whistle-blowing, near-miss report, acceptance of mistakes, can result in a sub-culture of cover-up and distraction from ethical values • Having a robust and well-known organizational model, system of values, code of conduct, it's key to have strong ethical organizational culture. • Whether the funds are coming from donors, government, internal solidarity, failure in using the funds for the purpose they are intended for may give the perception of unethical behavior.
Strategic	Strategical misunderstandings, governance unclarity and ineffectiveness.	• Failure of mutual understanding on strategical issues can result in frustration and strategic immobility. • Clarity and validation over governance mechanisms and functioning rules can help the organization to navigate firmly and transform threats into opportunities for growth and enrichment.

2. Risk Perimeters

The integration and the interactions between the Congregation OLCGS and GSIF are deep and constant, and it can be sometimes difficult to discern the risks perimeters. Some risks related to the Congregation might have a direct or indirect impact on GSIF and vice versa.

It is therefore important a good level of open-mindedness, flexibility, strategic-thinking, good communication skills and attitudes, at all levels.

Nevertheless, the perimeter of risks awareness to which this document refers to is GSIF and not the OLCGS.



3. Risk Tolerance

GSIF shall have the lowest tolerance for risks related to compliance (with administrative, financial and other rules, regulations, policies and procedures). GSIF has a ZERO-tolerance policy regarding child abuse (see GSIF Child Safeguarding Policy). GSIF is completely against fraud, bribery and corruption. GSIF's appetite for strategic, programmatic and operational risks shall be higher in order to meet the challenges faced in protecting the most vulnerable with the mix of caution, agility and innovation required to manage risk or exploit opportunities as appropriate. This implies that while sustaining its operations and meeting legal and ethical obligations shall be the highest priority for GSIF, all levels of the organization will demonstrate an informed risk-taking readiness to promote technical excellence.

> While meeting legal and ethical obligations shall be the highest priority for GSIF, all levels of the organization will demonstrate an informed risktaking readiness to promote technical excellence

4. Risk Ownership

The GSIF Risk Awareness Policy is based on the following principle: whoever is accountable for achieving a goal or for delivering a result is also responsible for assessing the risks associated with that goal or that result. Although the ultimate responsible for Risk Management in GSIF is the Board of Directors, who appoints a Risk Awareness Focal Point among its members, it is responsibility of whoever has management role to own a share of risk.

GSIF Risk Awareness Policy counts on two key-roles:

Risk Owner

is the person or the organizational body responsible for managing risks related to the objective he/she/it is accountable for. It means monitoring risks, proposing risk response and ensuring necessary actions are taken. That doesn't mean that the owner of a risk has authority over every decision or action that may change the level of the risk.

In GSIF there are 11 Risk Owners as follows:

- Assembly of Founders
- Board of Directors
- Director
- Latin America Regional Manager
- Asia Pacific Regional Manager
- Africa and Middle East Group Coordinator
- PCM Quality Desk Manager
- Communication and Fundraising Desk Manager
- Learning and Capacity Development Desk Manager
- Regional Working Group Coordinator
- Finance and Administration Desk Manager

Risk Focal Point

is the person responsible for gathering all the risk assessments at the different level (strategic and operational) of the organization and prepare the report to the Board of Directors. He/She does not have a managing role for Risk Management. In GSIF there are two Risk Awareness Focal Points as follows:

1. One at the strategic level:
   - Board Member appointed by the Board of Directors as Risk Awareness Focal Point;

2. One at the operational level:
   - CFO

5. Risk management process

The Risk Management Process consists of 5 steps coordinated by every Risk Owner for the specific area of competence:

1

Brainstorming and risks identification

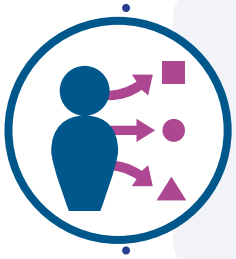
Looking at the relevant mandate (received either by Bylaws, Internal Regulation, Terms of Reference, Job Description, funder's expectations) and considering the internal and external contexts, the Risk Owner shall identify the risks for her/his/its area of competence, using the Risk Identification Template (see Risk Management Tools);

2

Risk assessment and evaluation

For every risk identified, the Risk Owner shall assess the potential impact by scoring the likelihood and the vulnerability. It shall be used the Risk Assessment Matrix (see Risk Management Tools);

3



Proposal of risks mitigation measures

The Risk Owner shall propose one or more risk mitigation measures for the risks identified and assessed. There are four possible reactions to a risk: accept, avoid, transfer or reduce.

4

Actions

The Risk Owner will make sure that the necessary actions are taken or transferred to the relevant management body.

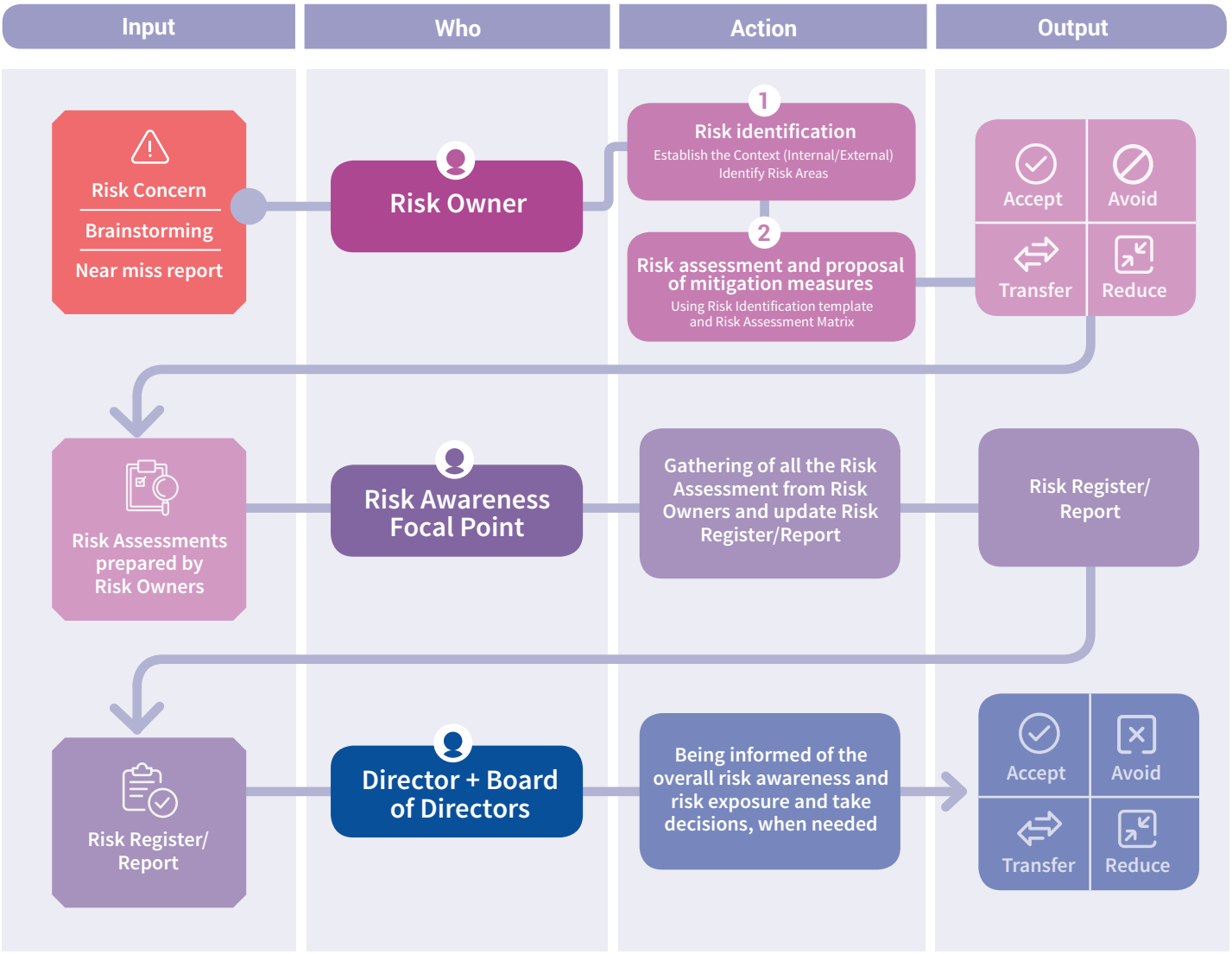
5

Monitoring and reporting

The Risk Owner is responsible for monitoring the evolution of the situation related to that or those risks and to revise the risk management action plan.

6. Risk Management Flowchart

Every Risk Owner should adopt the Risk Management Flowchart described below. For identifying the risks, every Risk Owner should consider internal and external context and factors and should refer to different type of Risk Areas (see page 7).
Given the deep integration and constant interactions between the Congregation OLCGS and GSIF, it is key to keep the relevant OLCGS partners involved and informed during the different steps of the Risk management process, as appropriate.



⚠ Risk Areas

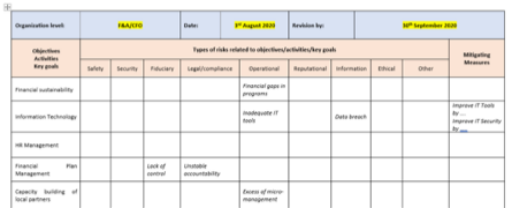
- **SAFETY AND SECURITY** (accident, illness, violence, crime)
- **FIDUCIARY** (inadequate financial controls against corruption/fraud/ theft/diversion)
- **LEGAL/COMPLIANCE** (violating laws or regulations of international or governments issues)
- **OPERATIONAL** (inability to achieve objectives, capacity/competence gaps, financial/funding constraints, access constraints)
- **REPUTATIONAL** (damage to image and reputation)
- **INFORMATION TECHNOLOGY** (data breach/loss digital risk)
- **ETHICAL** (risk of harm caused by unethical behaviors including sexual misconduct/exploitation, inadequate duty of care or insufficient consideration of humanitarian principles)
- **POLITICAL/STRATEGIC/ GOVERNANCE**

7. Risk Management

GSIF uses 4 Risk Management Tools

The Risk Identification Template

Is the main tool used by each Risk Owner for identifying the risks associated with her/his/its area of competence.



Risk Assessment Matrix

Is a tool used to assess the level of Risk (High, Medium, Low) by scoring the impact on GSIF of a potential risk and the likelihood that an event will occur. The Risk Assessment Matrix will help to understanding the level of urgency of taking actions.

Near miss report

A near miss is an unplanned event that did not result in injury or damage - but had the potential to do so. Identifying and reporting the near-misses is a key input for risk identification and assessment. **Whoever come in contact with a near miss should immediately report it by using the Near Miss Report without any fear of blame.**

Risk Register/Report

Is a repository or risk log of identified risks, which includes priority ratings, and risk response strategy. It is filled in by the two Risk Awareness Focal Points (Board Member appointed and CFO) for the two different levels (strategic and operational) and is submitted to the Board of Directors' meeting every year.

8. Risk Awareness Timeframe

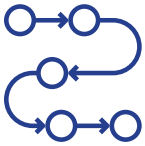
GSIF is committed to:

- **develop risk management skills and knowledge** among GSIF Staff and GSIF implementing partners. For this reasons, GSIF Risk Management Focal Points might organize during the year specific sessions for disseminating the GSIF risk awareness methodology and promoting a risk aware culture across the organization and the GS network.

- **encourage risk event reporting and whistle blowing:** during the year, at all time, GSIF encourage all levels of the organization to reporting risk events and risk concerns to the direct line manager/risk owner. Whoever come in contact with a near miss should immediately report it by using the Near Miss Report without any fear of blame.

9. Some risks of Risk Management

Here some examples on how Risk Awareness and Risk Management can become potentially dysfunctional:



Risk Management as a formal compliance issue:

Not integrating risk management in all the sectors and at all levels of the organization can easily turn risk management into a matter of compliance to a procedure and/or to some donors' requirements. But too many unpredicted events lead to unpredictable actions and expenses in a variety of areas: incident response, litigation, recovery, reputational issues, to name a few.

Risk Management as a handbrake

Too many security controls, bureaucracy, constant sense of vulnerability and fear, resistance to take responsibility by the Risk Owners, immobility/ push-back. Risk awareness should help an organization to go ahead with consciousness. Not to get stuck in fear.

Risk Management as an armor:

Just because an organization has implemented a sound risk awareness policy, it does not make that organization invulnerable.
Reckless risk-taking should be avoided in any case.

10. References

- https://nonprofitrisk.org/
- https://www.iso.org/iso-31000-risk-management.html
- Security Risk Management:
  a basic guide for smaller NGOs
  by EUROPEAN INTERAGENCY SECURITY FORUM

GOOD SHEPHERD
INTERNATIONAL
FOUNDATION
ONLUS