RISK MANAGEMENT POLICY & FRAMEWORK

A Practical Framework for Identifying, Assessing, Treating and Monitoring Organizational and Programme Risks

| July 2020 |

Document owner	Director General/ designated Risk Management Lead
Approval authority	Board of Directors / Governing Body
Version	1.0
Status	Draft for Board Review
Effective date	Upon Board approval
Review cycle	Annually, and after a major incident or material change
Applies to	All staff, volunteers, consultants, implementing partners and relevant contractors
Related documents	Finance, Procurement, Safeguarding/PSEA, HR, Security, Incident Reporting, Data Protection, MEAL and Partnership policies

Document Approval and Revision Control

Prepared by	Executive Director / Risk Management Lead	
Reviewed by	Management Team / Finance / Programme Leads	
Approved by	Board of Directors	
Next review date	Within 12 months of approval	

1.0	October 2026	Initial draft adapted for Silent Cry Foundation's humanitarian and development operations.	Pending

Contents

1. Purpose and objectives…….. 4

2. Scope and principles…….4

3. Definitions……5

4. Risk management governance and responsibilities…….5

5. Risk categories…….5

6. Risk appetite and escalation…….6

7. Risk management process……7

8. Risk assessment methodology…….8

9. Risk treatment and action plans……..9

10. Risk registers, incidents and assurance……9

11. Communication, training and documentation……..10

12. Monitoring, reporting and policy review……..10

1. Purpose and Objectives

Silent Cry Foundation (SCF) recognises that uncertainty can affect its ability to protect people, deliver quality humanitarian and development programmes, use resources responsibly and maintain the trust of communities, donors, partners and public authorities. This Policy establishes a consistent, proactive and documented approach to managing risks across the Foundation.

Risk management is part of sound governance and everyday decision-making. It should help SCF prevent avoidable harm, strengthen resilience, identify opportunities and make informed decisions—not merely complete a compliance form.

1.1 Objectives

- Identify and record material risks that may affect SCF's strategic objectives, people, programmes, assets, funding and reputation.
- Assess risks consistently using likelihood, impact and a standard 5×5 risk matrix.
- Assign clear risk owners, controls, treatment actions, deadlines and escalation routes.
- Protect children, adults at risk, staff, volunteers, communities and other affected people from harm, exploitation, abuse and retaliation.
- Strengthen financial stewardship, fraud prevention, procurement integrity, donor compliance and accountability to affected populations.
- Support continuity of operations and safe delivery in changing, insecure or emergency contexts.
- Ensure management and the Board receive timely, accurate information and assurance about significant risks.
- Capture lessons from incidents, complaints, near misses, evaluations and changing operating conditions.

2. Scope and Principles

This Policy applies to all SCF offices, programmes, projects, field activities and operations, including work delivered through local partners, consultants, suppliers and contractors where relevant. All personnel are responsible for recognising and reporting risks within their role.

2.1 Guiding principles

- Leadership and ownership: risks have named owners and are considered in planning, budgeting and operational decisions.
- Proportionality: controls and documentation reflect the severity and context of each risk.

- Prevention and do-no-harm: the safety, dignity, rights and wellbeing of communities and personnel take priority.
- Transparency and accountability: concerns are reported promptly and managed fairly, confidentially and without retaliation.
- Evidence-based decisions: ratings and treatment choices are supported by available information and professional judgement.
- Integration: risk management is embedded in programme design, MEAL, finance, procurement, safeguarding, security and partnership management.
- Continuous improvement: controls are reviewed after incidents, near misses, changes in context and lessons learned.
- Risk-aware innovation: opportunities may be pursued where benefits, safeguards and residual risks are understood and approved.

3. Definitions

Risk	The effect of uncertainty on SCF's objectives; it may create harm, loss, delay or an opportunity.
Inherent risk	The level of risk before considering existing controls.
Control	A policy, procedure, approval, system, physical measure or practice that reduces risk.
Residual risk	The level of risk remaining after existing controls and planned treatments are considered.
Risk appetite	The type and level of risk SCF is willing to accept while pursuing its objectives.
Risk owner	The manager or designated person accountable for monitoring a risk and ensuring actions are completed.
Risk register	The controlled record of significant risks, ratings, controls, owners, actions and review dates.
Risk treatment	Action to avoid, reduce, share/transfer or consciously accept a risk.
Incident / near miss	An event that caused harm or loss, or could reasonably have done so.
Safeguarding concern	A concern about actual, alleged or potential abuse, exploitation, neglect or other harm involving a person affected by SCF's work.

4. Governance and Responsibilities

Board of Directors	Approves this Policy and SCF's risk appetite; reviews strategic and high/extreme risks; challenges management on controls and overdue actions; ensures adequate resources and independent assurance.
Executive Director	Accountable for implementing the framework, promoting a risk-aware culture, assigning risk owners, escalating critical risks and reporting to the Board.
Risk Management Lead / designated focal point	Maintains the corporate risk register; coordinates assessments and reviews; monitors overdue actions; consolidates risk reports; supports training and policy compliance. This role may be assigned to an existing manager.
Programme / Project Managers	Identify programme and context risks; maintain project risk registers; assess partner and delivery risks; integrate mitigations into workplans and budgets; report changes and incidents.
Finance Manager	Manages financial control, cash, fraud, budget, donor financial compliance, fraud allegations, financial reporting and continuity risks.
Procurement / Logistics Lead	Manages supplier due diligence, competition, conflicts of interest, delivery, storage, asset security and procurement integrity risks.
HR / Safeguarding / Security focal points	Manage risks within their mandates, including staff duty of care, safeguarding/PSEA, safe recruitment, security, incident response and confidential referral pathways.
MEAL / Data focal point	Supports risk indicators, data quality, secure information management, feedback analysis and evidence that mitigation measures are working.
Implementing partners and contractors	Comply with relevant contractual and policy requirements; report material risks and incidents promptly; maintain appropriate controls and cooperate with due diligence and monitoring.
All personnel and volunteers	Follow controls, raise concerns promptly, participate in training and never conceal or retaliate against good-faith risk reporting.

SCF may establish a management Risk Review Group or assign the review function to an existing management meeting. If a separate committee is not practical, the Executive Director must document how risk review, escalation and Board reporting will be carried out.

5. Risk Categories

- Strategic and governance: failure to meet mission, strategy, sustainability, governance or stakeholder commitments.
- Programme quality and delivery: weak needs assessment, poor targeting, implementation delays, ineffective activities or unintended harm.
- Safeguarding and PSEA: child safeguarding, sexual exploitation and abuse, harassment, abuse of power, unsafe referrals or retaliation.
- Security, access and duty of care: conflict, violence, travel, detention, civil unrest, mines/UXO, natural hazards or unsafe field conditions.
- Financial and fraud: theft, fraud, corruption, bribery, cash loss, unauthorised expenditure, currency fluctuations or weak segregation of duties.
- Procurement, logistics and assets: collusion, conflicts of interest, poor-quality goods, supplier failure, stock loss, diversion or asset misuse.
- Legal, regulatory and donor compliance: registration, permits, employment obligations, donor restrictions, reporting deadlines or contractual breaches.
- Partner and third-party: weak partner capacity, misconduct, inadequate controls, delivery failure or sub-grant misuse.
- People and organisational capacity: turnover, skills gaps, staff wellbeing, misconduct, workplace safety or inadequate succession.
- Data protection and information security: unauthorised access, loss, disclosure, unsafe collection of personal data or cyberattack.
- Reputation, communications and community trust: misinformation, poor complaints handling, perceived bias, unmet commitments or harmful public statements.
- Environmental, climate and social: environmental damage, climate shocks, exclusion, conflict sensitivity or unintended negative community impacts.
- Business continuity and technology: power, connectivity, system failure, office disruption, loss of records or inability to operate.

6. Risk Appetite and Escalation

The Board sets SCF's risk appetite and reviews it at least annually. Until the Board formally approves a risk appetite statement, the following interim approach applies:

Safeguarding, PSEA, abuse, exploitation, retaliation and deliberate harm	Very low. No deliberate tolerance; concerns must be reported and managed through safeguarding procedures.
Fraud, bribery, corruption, deliberate misuse of funds or falsification	Very low. Suspected cases must be escalated promptly and handled under applicable investigation and reporting procedures.
Legal, donor and contractual compliance	Low. Any potential material breach must be escalated to the Executive Director and relevant lead without delay.
Staff, volunteer and community safety	Low. Activities must be paused or changed where risks are unacceptable and cannot be adequately controlled.
Programme delivery, finance, operations and reputation	Low to moderate, depending on context, controls and the potential impact on people and mission.
Innovation and strategic opportunities	Considered case by case, with documented benefits, safeguards, approvals and residual-risk acceptance.

6.1 Escalation requirements

- Any suspected safeguarding/PSEA incident, serious security event, suspected fraud/corruption, major data breach, death/serious injury or credible threat to life must be escalated immediately through the applicable incident protocol. Do not wait for the next routine risk review.
- High and extreme risks must be reported promptly to the Executive Director and relevant risk owner, with immediate interim controls and a documented action plan.
- Moderate risks require a named owner, proportionate treatment and regular management review.
- Low risks may be managed at operational level but must still be recorded where recurring, cross-cutting or relevant to a programme objective.
- Only the authority delegated by the Board may formally accept a high or extreme residual risk. Acceptance does not override law, donor rules or safeguarding obligations.

7. Risk Management Process

1. Establish the context: confirm objectives, operating environment, stakeholders, assumptions and legal/donor requirements.
2. Identify risks: use staff and partner consultations, community feedback, incident and complaints trends, security updates, assessments, audits, MEAL findings and scenario planning.
3. Analyse risks: identify causes, possible consequences, existing controls and their effectiveness; score likelihood and impact.
4. Evaluate and prioritise: compare scores against the matrix and risk appetite; identify what requires escalation or further treatment.
5. Treat risks: select practical controls, assign an owner, budget and deadline, and define how completion and effectiveness will be verified.
6. Communicate and consult: share relevant risk information with staff, partners, affected communities and donors where appropriate, while protecting confidentiality.
7. Monitor and review: update ratings and actions as conditions change; review after incidents, near misses, project changes or new evidence.
8. Record and learn: maintain the risk register and evidence of decisions; share lessons and incorporate them into future design and operations.

7.1 When risk assessments are required

- During annual strategy, budget and workplan development.
- At proposal development and before launching a new project, activity, site or partnership.
- Before high-risk travel, distributions, cash transfers, procurement or work in insecure locations.
- During partner selection and before signing or materially changing an agreement.
- After a significant incident, complaint trend, audit finding, context change or near miss.
- At scheduled project and corporate risk reviews.

8. Risk Assessment Methodology

SCF uses a 5×5 qualitative risk matrix. Assess likelihood and consequence on a scale of 1 to 5. Risk score = Likelihood × Consequence. Rate the risk using the highest credible consequence, considering effects on people, programme objectives, finances, compliance, reputation, environment and continuity.

1	Rare	Would be exceptional; not expected in normal circumstances.
2	Unlikely	Could happen, but is not expected to occur in most circumstances.
3	Possible	Might occur at some point or has occurred in comparable settings.
4	Likely	Expected to occur in many circumstances or has occurred repeatedly.
5	Almost certain	Expected to occur frequently or is already occurring.

1	Negligible	Minimal disruption or loss; no significant harm; quickly managed locally.
2	Minor	Limited and reversible impact; minor injury, delay, complaint or cost.
3	Moderate	Material programme disruption, reportable incident, moderate financial loss or significant corrective action.
4	Major	Serious harm, substantial service interruption, major donor/compliance issue, significant financial loss or lasting reputational damage.
5	Catastrophic	Death or life-threatening harm, widespread serious abuse, major fraud, severe legal consequences, loss of critical funding or prolonged inability to operate.

8.1 Risk score bands

Score	Level	Required response
1–9	Low	Manage through routine controls; monitor at team/project level.
10–12	Moderate	Document treatment actions; manager review and regular follow-up.
15–25	High	Prompt treatment and escalation to the Executive Director; regular senior management oversight.

Note: The supplied reference policy uses the same bands. The 5×5 multiplication matrix produces no scores of 13 or 14. Any safeguarding, serious security, suspected fraud or potential legal breach must be escalated based on its nature, even if its numerical score is lower.

8.2 Inherent and residual risk

Record the inherent score before controls where useful, assess the effectiveness of current controls, then record the residual score after those controls. Re-score after treatment actions are completed and evidence shows they work. Do not lower a rating solely because an action has been planned.

8.3 Control effectiveness

Effective	Controls are documented, understood, operating and supported by evidence.
Partially effective	Some controls work, but gaps or inconsistent implementation remain.
Ineffective / absent	Controls are missing, not followed or do not provide reasonable assurance.

9. Risk Treatment and Action Plans

The risk owner selects treatment measures in consultation with relevant staff and stakeholders. Options include:

- Avoid: stop or redesign the activity that creates unacceptable risk.
- Reduce: add preventive or detective controls, change procedures, improve training, strengthen supervision or adjust delivery methods.
- Share or transfer: allocate responsibilities through insurance, contracts or partnership arrangements where lawful and appropriate; SCF remains accountable for its own obligations.
- Accept and monitor: accept only within approved risk appetite and delegated authority, with a documented rationale and review date.
- Exploit or enhance an opportunity: where a positive opportunity is identified, document the expected benefit, costs, safeguards and decision authority.

9.1 Minimum action plan fields

- Action and expected outcome
- Named individual accountable for delivery

- Due date and required resources/budget
- Interim controls pending completion
- Evidence that the action is complete
- Method and date for testing effectiveness
- Residual score and approval of any residual-risk acceptance

Overdue actions on high risks must be escalated to the Executive Director. Where actions cannot be completed on time, the owner must document the reason, interim controls, revised deadline and approval.

10. Risk Registers, Incidents and Assurance

10.1 Risk registers

SCF will maintain a corporate risk register and project/department registers proportionate to its size and portfolio. Registers should be secure, version-controlled and accessible only to authorised personnel. Personal, safeguarding, security-sensitive or investigation details must not be placed in a general register; use a restricted record and cross-reference it using a non-sensitive identifier.

Each entry should record a unique ID, date, objective, risk statement, causes, consequences, category, existing controls, inherent score where used, residual likelihood and impact, score, level, owner, treatment actions, deadline, status, escalation, last review and next review.

10.2 Incident and near-miss management

When a risk materialises, staff must prioritise immediate safety and follow SCF's relevant incident, safeguarding, security, fraud, HR or data-breach procedure. Report and document the incident through the approved channel. Assess whether the event indicates a recurring or wider organisational risk. Keep the risk open where recurrence is possible or underlying causes remain; close it only when the risk is no longer relevant or is adequately controlled and the decision is documented.

10.3 Assurance

Management should use proportionate evidence to verify controls, including budget reviews, reconciliations, procurement checks, partner monitoring, field visits, safeguarding audits, security briefings, MEAL data quality checks, complaint trend analysis and internal/external audit findings. Significant control gaps must have a corrective action owner and deadline.

10.4 Risk reporting

Monthly	Project and departmental owners review significant risks, new risks, incidents, controls and overdue actions.
Quarterly	Management reviews the corporate register, high risks, risk trends, risk appetite exceptions and treatment progress.
At least every six months	Board receives a summary of strategic/high risks, changes in exposure, major incidents, overdue actions and assurance gaps.
Immediately / ad hoc	Material safeguarding, security, fraud, data, legal or operational incidents and any rapidly escalating high/extreme risk are escalated without waiting for scheduled reporting.

11. Communication, Training and Documentation

- The policy and approved templates must be made available to relevant personnel and explained during induction.
- Risk owners and managers must receive practical guidance on scoring, treatment, escalation and updating registers.
- Partners and contractors must be informed of applicable requirements through agreements, onboarding and monitoring.
- Risk information must be shared on a need-to-know basis. Confidentiality must not be used to conceal misconduct or prevent required reporting.
- Risk decisions, approvals, treatment evidence, incident references and review dates must be documented and retained under SCF's records-retention rules and donor/legal obligations.

12. Monitoring, Compliance and Review

The Director General and designated Risk Management Lead will monitor implementation. Non-compliance may result in corrective action and, where appropriate, disciplinary, contractual or legal action in accordance with applicable procedures. No person should suffer retaliation for raising a concern in good faith.

The Board will review this Policy at least annually. An earlier review is required after a serious incident, significant organisational change, material legal/donor change, audit finding or evidence that the framework is not effective. Superseded versions must be archived and clearly marked obsolete.

Related policies and procedures

- Safeguarding and Child Protection Policy
- Protection from Sexual Exploitation and Abuse (PSEA) Policy
- Security and Duty of Care Procedures
- Incident Reporting and Response Procedure
- Fraud, Anti-Bribery and Whistleblowing Policy
- Finance and Procurement Policies
- HR and Code of Conduct
- Data Protection / Information Security Procedure
- MEAL Policy and Complaints & Feedback Mechanism
- Partner Due Diligence and Agreement Procedures

Approved date July 2020