Safeguarding Risk Register

	Name (Event)	Likelihood	Impact	Comments
Risk ID1:	Staff member engages in sexual exploitation or abuse of beneficiaries	Low	Major	
Mitigation	**Action**		**Timeline**	
Action 1	Immediate investigation		Immediate	
Action 2	Increase field monitoring and refresher training		Annually	
Action 3	Review/update SG Policy		Every 2 years	
Insert row to add action				

	Name (Event)	Likelihood	Impact	Comments
Risk ID2:	Retaliation against whistleblowers	Low	Major	
Mitigation	**Action**		**Timeline**	
Action 1	Conduct awareness sessions on protection measures		Annually	
Insert row to add action				

	Name (Event)	Likelihood	Impact	Comments
Risk ID3:	Confidential survivor information is improperly disclosed	Low	Major	
Mitigation	**Action**		**Timeline**	
Action 1	Strengthen secure data storage and access controls		Work in progress	
Insert row to add action				

Fraud and Corruption Risk Register

	Name (Event)	Likelihood	Impact	Comments
Risk ID1:	Fake or inflated invoices submitted by vendors	Low	Major	
Mitigation	**Action**		**Timeline**	
Action 1	Implementation of the payment and voucher verification policy and four-eyes principle.		In place	
Action 2	Conduct spot checks and vendor verification		Annually	
Insert row to add action				

	Name (Event)	Likelihood	Impact	Comments
Risk ID2:	Procurement staff receive bribes or kickbacks	Low	Major	
Mitigation	**Action**		**Timeline**	
Action 1	Segregation of duties in procurement, vendor selection, payment approval, and contract management processes.		In place	
Action 2	Periodically monitor repeated awards to the same vendor to detect any indication of bribery, kickbacks, or conflict of interest.		Every 6 months	
Action 3	Provide regular ethics, safeguarding, and anti-corruption training to staff.		Annually	
Insert row to add action				

	Name (Event)	Likelihood	Impact	Comments
Risk ID3:	Fraudulent emails purportedly sent from donors requesting refunds of alleged wrong payments or requesting fund transfer to different bank accounts.	Low	Major	
Mitigation	**Action**		**Timeline**	
Action 1	Establish clear procedures for identifying suspicious emails, including verification of sender addresses, and unusual requests.		In place	
Action 2	Staff awareness training on phishing, spoofed emails, and cyber fraud risks.		Annually	
Insert row to add action				