- **Burmese Community Development Collaboration (BCDC)**

RISK MANAGEMENT POLICY

Version 2.0
Reviewed on May 2027

BCDC
BURMESE COMMUNITY
DEVELOPMENT COLLABORATION

Table of Contents

1. Introduction

The Burmese Community Development Collaboration (BCDC) is committed to maintaining a strong culture of accountability, safeguarding, integrity, transparency, and responsible governance across all areas of its work. As a community-based organisation operating in humanitarian, development, settlement support, aged care, advocacy, and community empowerment contexts, BCDC recognises that effective risk management is essential to protecting the people and communities it serves, safeguarding organisational resources, ensuring legal and ethical compliance, and sustaining long-term organisational effectiveness.

BCDC operates across diverse and, at times, complex operational environments, including Australia, Myanmar, Thailand border areas, and other regional contexts affected by displacement, conflict, humanitarian crises, social vulnerability, and rapidly changing political and security conditions. The organisation acknowledges that these operational contexts may expose BCDC, its personnel, partners, volunteers, and stakeholders to a wide range of risks, including safeguarding risks, financial misconduct, operational disruptions, security threats, reputational harm, legal liabilities, cybersecurity threats, fraud and corruption, partnership risks, and risks associated with humanitarian and cross-border activities.

BCDC recognises that unmanaged or poorly managed risks can negatively impact:

- The safety, dignity, and wellbeing of children, vulnerable individuals, communities, staff, volunteers, and partners;
- The quality, effectiveness, and continuity of programs and services;
- Organisational reputation, credibility, and stakeholder trust;
- Financial sustainability and donor confidence;
- Legal and regulatory compliance obligations;
- The organisation's ability to fulfil its mission, values, and strategic objectives.

This Risk Management Policy establishes BCDC's organisation-wide framework for identifying, assessing, managing, monitoring, mitigating, and reviewing risks that may affect organisational operations, governance, programs, partnerships, personnel, assets, information systems, and external relationships.

Through the implementation of this Risk Management Policy, BCDC seeks to strengthen organisational resilience, support safe and effective programming, promote accountability and transparency, protect stakeholders and communities from harm, and ensure the long-term sustainability and integrity of the organisation and its mission.

The policy is intended to support proactive, informed, and responsible decision-making at all levels of the organisation. It promotes a prevention-focused and risk-informed organisational culture in which risk management is integrated into governance, strategic planning, safeguarding systems, financial management, program implementation, partnership engagement, operational planning, and continuous improvement processes.

BCDC understands that risk management is not solely the responsibility of senior leadership or the Board, but a shared organisational responsibility. All personnel associated with BCDC — including Board members, employees, volunteers, contractors, consultants, interns, and partner organisations — are expected to actively contribute to identifying, reporting, and managing risks within their areas of responsibility.

This policy also reflects BCDC's commitment to complying with:

- The ACFID Code of Conduct;
- Australian Charities and Not-for-profits Commission (ACNC) External Conduct Standards;
- Relevant Australian laws and regulatory obligations;
- Safeguarding and protection obligations;
- DFAT counter-terrorism and sanctions requirements;
- Privacy and confidentiality standards;
- International humanitarian and development good practice principles.

BCDC further recognises that risk management is an ongoing and evolving process. Risks may change over time due to shifts in political conditions, humanitarian emergencies, funding environments, technology, organisational growth, partnership arrangements, or operational contexts. Accordingly, BCDC is committed to regularly reviewing and strengthening its risk management systems, policies, procedures, and organisational capacities to ensure that risks are appropriately identified and managed in a timely, ethical, and accountable manner.

2. Purpose of the Policy

The purpose of this Risk Management Policy is to establish a comprehensive and organisation-wide framework for identifying, assessing, managing, monitoring, mitigating, and reviewing risks that may affect the Burmese Community Development Collaboration (BCDC), its personnel, programs, partnerships, assets, operations, beneficiaries, and stakeholders.

This policy aims to ensure that risk management is embedded into all levels of organisational governance, strategic planning, decision-making, safeguarding practices, operational management, financial oversight, partnership engagement, and program implementation. BCDC recognises that effective risk management is essential to maintaining organisational integrity, accountability, sustainability, legal compliance, and the safety and wellbeing of all individuals connected to its work.

The policy is designed to support BCDC in:

- Protecting children, vulnerable adults, communities, staff, volunteers, partners, and stakeholders from harm, abuse, exploitation, neglect, discrimination, and other forms of risk;
- Preventing, reducing, and responding appropriately to operational, safeguarding, financial, legal, reputational, cybersecurity, partnership, environmental, and security-related risks;
- Strengthening organisational resilience, preparedness, and continuity during emergencies, crises, humanitarian responses, or unstable operational conditions;
- Supporting informed, ethical, transparent, and risk-aware decision-making processes across the organisation;
- Ensuring that risks are identified and addressed proactively rather than reactively;
- Promoting accountability and shared responsibility for risk management among Board members, management, staff, volunteers, and partner organisations;
- Protecting organisational assets, information, financial resources, systems, and public trust;
- Supporting compliance with the ACFID Code of Conduct, Australian laws and regulations, safeguarding obligations, DFAT counter-terrorism requirements, and other relevant governance standards;
- Strengthening confidence among donors, beneficiaries, partners, regulators, and community stakeholders regarding BCDC's governance and operational systems;
- Improving organisational learning, adaptive management, and continuous improvement through systematic monitoring and review of risks and mitigation measures.

This policy also seeks to provide clear guidance on:

- How risks are identified, assessed, documented, escalated, and managed;
- Roles and responsibilities relating to risk management;
- Risk reporting and incident response procedures;
- Governance oversight and accountability mechanisms;
- The integration of safeguarding, due diligence, and financial integrity measures into organisational risk management systems.

BCDC recognises that its operational environments may involve heightened and evolving risks, particularly in humanitarian, displacement, conflict-affected, cross-border, and community-based contexts. Accordingly, this policy is intended to support consistent, proportionate, context-sensitive, and prevention-focused approaches to managing risk across all organisational activities.

Ultimately, the purpose of this policy is to strengthen BCDC's ability to fulfil its mission safely, ethically, effectively, and sustainably while protecting the rights, dignity, wellbeing, and trust of the communities and stakeholders it serves.

3. Organisational Commitment to Risk Management

The Burmese Community Development Collaboration (BCDC) is committed to fostering a strong organisational culture of accountability, safeguarding, ethical conduct, transparency, and responsible risk management across all aspects of its operations, governance, partnerships, and program activities.

BCDC recognises that effective risk management is fundamental to achieving its mission, protecting the communities and individuals it serves, ensuring organisational sustainability, maintaining stakeholder trust, and supporting safe, inclusive, and effective service delivery. The organisation therefore commits to integrating risk management into all organisational systems, operational processes, strategic planning activities, and decision-making frameworks.

BCDC acknowledges that risks exist in all areas of organisational work, including humanitarian and development programming, community engagement, safeguarding, financial management, partnerships, overseas operations, digital systems, volunteer engagement, and advocacy activities. The organisation further recognises that some operational environments — particularly those involving conflict-affected regions, displacement settings, humanitarian emergencies, and vulnerable populations — may involve elevated and rapidly changing risks requiring heightened oversight and context-sensitive responses.

In fulfilling its commitment to effective risk management, BCDC commits to:

- Promoting a proactive and prevention-focused approach to identifying and managing risks before they result in harm or operational disruption;
- Embedding risk management principles into organisational governance, program design, operational planning, financial oversight, safeguarding systems, partnership management, and monitoring processes;
- Ensuring that the safety, dignity, wellbeing, and rights of children, vulnerable adults, communities, staff, volunteers, and stakeholders remain central to all risk management decisions;
- Maintaining systems and procedures that support timely identification, reporting, escalation, investigation, mitigation, and monitoring of risks and incidents;
- Allocating appropriate organisational oversight, leadership attention, and resources to support effective risk management practices;
- Strengthening organisational resilience and preparedness to respond to crises, emergencies, operational disruptions, safeguarding concerns, security incidents, and other unforeseen events;

- Supporting ethical, transparent, evidence-informed, and accountable decision-making processes at all levels of the organisation;
- Ensuring that risk management responsibilities are clearly understood and shared by Board members, management, staff, volunteers, contractors, consultants, and partner organisations;
- Supporting a culture in which individuals feel safe and encouraged to report risks, concerns, incidents, misconduct, safeguarding issues, financial wrongdoing, or unethical behaviour without fear of retaliation;
- Conducting due diligence and proportionate risk assessments prior to entering partnerships, funding arrangements, overseas activities, or high-risk operational engagements;
- Implementing reasonable safeguards to protect organisational assets, confidential information, financial resources, digital systems, and stakeholder data;
- Continuously reviewing and improving organisational risk management systems in response to operational learning, environmental changes, stakeholder feedback, incidents, audit findings, and evolving legal or regulatory requirements.

BCDC is also committed to ensuring that its risk management systems align with:

- The ACFID Code of Conduct;
- Australian Charities and Not-for-profits Commission (ACNC) requirements;
- Relevant Australian legal and regulatory obligations;
- DFAT safeguarding, counter-terrorism, and sanctions requirements;
- Privacy, confidentiality, and information security obligations;
- International humanitarian and development good practice standards.

The BCDC Board and organisational leadership recognise that effective risk management is essential to good governance and organisational sustainability. The Board therefore commits to providing oversight of organisational risks, supporting the development of appropriate risk management systems, reviewing significant risks and mitigation measures, and ensuring that risk management remains integrated into strategic and operational planning processes.

BCDC further recognises that risk management is an ongoing and evolving process rather than a one-time activity. As organisational contexts, operational environments, partnerships, technologies, and humanitarian conditions change over time, BCDC commits to maintaining flexible, adaptive, and continuously improving risk management systems capable of responding to emerging and evolving risks.

Through this commitment, BCDC seeks to strengthen organisational integrity, improve operational effectiveness, support safe and accountable programming, protect stakeholders and communities from harm, and ensure the long-term sustainability and credibility of the organisation and its mission.

4. Scope and Application

This Risk Management Policy applies to all activities, operations, governance functions, partnerships, personnel, and programs undertaken, funded, coordinated, supported, or represented by the Burmese Community Development Collaboration (BCDC), both within Australia and internationally.

The policy establishes an organisation-wide framework for managing risks across all levels of BCDC's work and is intended to ensure that risk management considerations are consistently integrated into organisational governance, safeguarding, strategic planning, operational management, financial oversight, partnership engagement, humanitarian response activities, and community service delivery.

This policy applies to all individuals and entities associated with BCDC, including but not limited to:

4.1 Board Members and Governance Representatives

All members of the BCDC Board, advisory groups, governance committees, and organisational leadership structures are required to comply with this policy and fulfil their responsibilities relating to risk oversight, governance accountability, strategic decision-making, and organisational stewardship.

4.2 Employees and Staff Members

This policy applies to all BCDC employees, including:

- Full-time staff;
- Part-time staff;
- Casual staff;
- Temporary personnel;
- Remote workers;
- Field-based staff;
- Program coordinators;
- Administrative and operational staff.

All staff members are expected to actively participate in identifying, reporting, mitigating, and managing risks within their areas of responsibility.

4.3 Volunteers, Interns, and Community Representatives

This policy applies to all volunteers, interns, community focal persons, and informal representatives involved in BCDC activities, regardless of the duration, location, or nature of their engagement.

Volunteers and community representatives are expected to:

- Follow risk management procedures;
- Report risks or incidents promptly;
- Participate in safeguarding and safety practices;
- Contribute to maintaining safe and ethical operational environments.

4.4 Contractors, Consultants, and Service Providers

All contractors, consultants, suppliers, facilitators, trainers, interpreters, and external service providers engaged by BCDC are required to operate in accordance with this policy and any relevant organisational risk management procedures, safeguarding requirements, and compliance obligations.

BCDC may conduct due diligence and risk assessments prior to engaging external individuals or organisations.

4.5 Partner Organisations and Collaborative Entities

This policy applies to partner organisations, implementing partners, community-based organisations, diaspora groups, networks, consortium members, referral partners, and collaborating entities involved in BCDC-supported activities or programs.

BCDC expects all partners to:

- Uphold appropriate safeguarding and risk management standards;
- Participate in due diligence and risk assessment processes;
- Cooperate with monitoring, reporting, and accountability mechanisms;
- Take reasonable measures to identify and manage operational risks.

The level of oversight and monitoring may vary depending on:

- The nature of the partnership;
- Funding arrangements;
- Geographic and operational contexts;
- Risk levels associated with the activities.

4.6 Geographic Scope

This policy applies to all BCDC activities conducted:

- Within Australia;
- In Myanmar;
- In Thailand border areas;
- In cross-border humanitarian contexts;
- In any other country or operational location where BCDC conducts, supports, funds, coordinates, or participates in activities.

BCDC recognises that different operational environments may involve different levels and types of risk. Accordingly, risk management approaches may be adapted to reflect:

- Local context;
- Security conditions;
- Humanitarian situations;
- Legal and regulatory environments;
- Cultural considerations;
- Safeguarding vulnerabilities;
- Access and logistical constraints.

4.7 Operational Scope

This policy applies across all areas of BCDC's work, including but not limited to:

- Humanitarian assistance and emergency response activities;
- Community development programs;
- Settlement support and refugee assistance;
- Aged care and community care services;
- Safeguarding and protection activities;
- Advocacy and community engagement;
- Education and training initiatives;
- Volunteer management activities;
- Financial management and fundraising;
- Procurement and resource management;
- Monitoring, evaluation, accountability, and learning activities;
- Digital communications and information management systems;
- Public communications, media engagement, and online platforms.

4.8 Application Throughout the Program and Organisational Cycle

Risk management considerations are expected to be integrated throughout all stages of organisational and program activities, including:

- Strategic planning;
- Program design;
- Partner selection and due diligence;
- Budgeting and procurement;
- Recruitment and onboarding;
- Program implementation;
- Monitoring and evaluation;
- Incident response;
- Reporting and review;
- Partnership management;
- Project closure and transition processes.

4.9 Relationship with Other Policies

This policy should be read and applied together with other relevant BCDC governance, safeguarding, operational, financial, and accountability policies and procedures, including:

- Child Safeguarding Policy;
- PSEAH Policy;
- Financial Wrongdoing Policy;
- Complaint Handling Policy;
- PMEL Policy;
- Partnership Commitment Policy;
- Privacy Policy;
- Human Resources Management Policy;
- Volunteer Manual;
- Code of Conduct;
- Non-Development Activity Policy;
- Environmental Sustainability and Climate Action Policy.

Where inconsistencies arise, BCDC will apply the approach that best protects the safety, rights, wellbeing, and integrity of affected individuals and organisational operations while maintaining compliance with relevant legal and regulatory obligations.

4.10 Compliance with the Policy

Compliance with this policy is mandatory for all individuals and entities covered under its scope.

Failure to comply with this policy, associated procedures, or organisational risk management requirements may result in:

- Disciplinary action;
- Suspension of duties or activities;
- Termination of employment, volunteer engagement, or partnership arrangements;
- Referral to relevant authorities where appropriate;
- Other corrective actions deemed necessary by BCDC.

BCDC reserves the right to monitor compliance with this policy and implement corrective or preventative actions where risks, non-compliance, or operational concerns are identified.

5. Definitions and Key Concepts

This section provides definitions and explanations of key terms used throughout this Risk Management Policy. These definitions are intended to support a shared understanding of risk management concepts across all areas of BCDC's governance, operations, partnerships, safeguarding systems, and program activities.

5.1 Risk

Risk refers to the possibility that an event, action, situation, or circumstance may negatively affect BCDC's ability to achieve its objectives, fulfil its obligations, protect individuals from harm, maintain organisational integrity, or deliver programs effectively and safely.
Risks may arise from internal or external factors and may impact:

- Individuals and communities;
- Organisational operations;
- Financial resources;
- Safeguarding responsibilities;
- Partnerships;
- Legal compliance;
- Reputation and stakeholder trust.

5.2 Risk Management

Risk management refers to the systematic and ongoing process of identifying, assessing, analysing, managing, monitoring, and reviewing risks that may affect BCDC's activities, operations, programs, personnel, partnerships, or stakeholders.
Risk management also includes implementing appropriate prevention, mitigation, response, and monitoring measures to reduce the likelihood or impact of harm or organisational disruption.

5.3 Risk Assessment

Risk assessment refers to the structured process of evaluating:

- The likelihood of a risk occurring; and
- The potential impact or consequences if the risk occurs.

Risk assessments help determine appropriate mitigation measures and decision-making responses.

5.4 Risk Mitigation

Risk mitigation refers to actions or measures taken to reduce:

- The likelihood of a risk occurring;
- The severity of potential harm;
- Operational disruption;
- Negative consequences associated with identified risks.

Mitigation measures may include:

- Safeguards;
- Internal controls;
- Policies and procedures;
- Training;
- Supervision;
- Monitoring systems;
- Security measures;
- Contingency planning.

5.5 Residual Risk

Residual risk refers to the level of risk that remains after mitigation measures or controls have been implemented.

BCDC recognises that not all risks can be fully eliminated and that some residual risks may remain within acceptable organisational tolerance levels.

5.6 Risk Register

A Risk Register is a formal organisational document used to record:

- Identified risks;
- Risk ratings;
- Existing controls;
- Mitigation measures;
- Responsible persons;
- Monitoring actions;
- Review dates.

The Risk Register supports ongoing organisational oversight and accountability.

5.7 Incident

An incident refers to any event, occurrence, allegation, concern, accident, breach, or situation that:

- Causes harm;
- Creates risk of harm;
- Disrupts operations;
- Violates organisational policies;
- Threatens the safety, wellbeing, rights, or security of individuals or organisational systems.

Incidents may include:

- Safeguarding concerns;
- Fraud allegations;
- Security incidents;
- Data breaches;
- Workplace injuries;
- Misconduct;
- Operational failures.

5.8 Safeguarding

Safeguarding refers to the responsibilities, policies, procedures, and actions taken to prevent and respond to:

- Abuse;
- Exploitation;
- Neglect;
- Harassment;
- Harm;
- Violence;
- Unsafe practices.

Safeguarding applies to children, vulnerable adults, beneficiaries, communities, staff, volunteers, and stakeholders.

5.9 Financial Wrongdoing

Financial wrongdoing refers to any dishonest, unethical, unlawful, or improper financial activity, including:

- Fraud;
- Corruption;
- Bribery;
- Theft;
- Embezzlement;
- Misuse of organisational resources;
- Money laundering;
- Financial misconduct.

5.10 Due Diligence

Due diligence refers to the process of gathering and assessing information before entering into partnerships, funding arrangements, procurement activities, or operational engagements to ensure:

- Ethical conduct;
- Legal compliance;
- Safeguarding suitability;
- Financial integrity;
- Alignment with BCDC values and obligations.

5.11 Prohibited Entities

Prohibited entities refer to organisations, groups, or individuals subject to:

- Sanctions;
- Counter-terrorism restrictions;
- Criminal prohibitions;
- Government restrictions;
- International sanctions regimes.

BCDC may conduct reasonable screening against relevant sanctions and prohibited entities lists during due diligence processes.

5.12 High-Risk Activity

High-risk activity refers to any operational activity, travel, engagement, or program context that may involve elevated risk to:

- Safety;
- Security;
- Safeguarding;
- Legal compliance;
- Organisational reputation;
- Financial integrity;
- Operational continuity.

Examples may include:

- Travel to conflict-affected areas;
- Humanitarian emergency response;
- Cross-border operations;
- Activities involving vulnerable populations.

5.13 Stakeholders

Stakeholders refer to individuals, groups, or entities that interact with, are affected by, or have an interest in BCDC's work.

Stakeholders may include:

- Beneficiaries;
- Communities;
- Staff;
- Volunteers;
- Partners;
- Donors;
- Government agencies;
- Regulators;
- Community leaders;
- Service providers.

6. Guiding Principles of Risk Management

BCDC's risk management approach is guided by principles that promote accountability, safeguarding, ethical conduct, transparency, prevention, and continuous improvement across all organisational activities.

6.1 Accountability and Shared Responsibility

BCDC recognises that effective risk management is a shared organisational responsibility.
All Board members, staff, volunteers, contractors, consultants, and partner organisations are expected to actively contribute to identifying, reporting, managing, and mitigating risks within their areas of responsibility.

6.2 Prevention and Early Intervention

BCDC prioritises proactive and prevention-focused approaches to risk management.
The organisation seeks to identify and address risks at an early stage before harm, operational disruption, financial loss, safeguarding failures, or reputational damage occur.

6.3 Safeguarding and Protection

The safety, dignity, rights, and wellbeing of children, vulnerable individuals, communities, staff, and stakeholders remain central to all risk management decisions and processes.
Safeguarding considerations must be integrated into:

- Program planning;
- Recruitment;
- Partnerships;
- Travel;
- Community engagement;
- Operational decision-making.

6.4 Transparency and Ethical Conduct

BCDC is committed to promoting honesty, integrity, openness, and ethical conduct in all risk management activities.
Risk management processes should be:

- Fair;
- Documented;
- Evidence-informed;
- Accountable;
- Consistent with organisational values and legal obligations.

6.5 Inclusiveness and Participation

Where appropriate, BCDC seeks to involve affected stakeholders, communities, staff, volunteers, and partners in identifying and understanding risks that may affect them.

The organisation recognises the importance of local knowledge, lived experience, and community participation in strengthening risk awareness and mitigation.

6.6 Context-Sensitive and Proportionate Approaches

BCDC recognises that risks vary across operational environments, geographic locations, partnership arrangements, and program activities.

Risk management responses should therefore be:

- Context-sensitive;
- Practical;
- Proportionate to the level of risk;
- Adaptable to changing circumstances.

6.7 Continuous Learning and Improvement

BCDC is committed to continuously strengthening its risk management systems through:

- Monitoring and review;
- Lessons learned;
- Incident analysis;
- Stakeholder feedback;
- Training and capacity building;
- Policy review processes.

6.8 Legal and Regulatory Compliance

Risk management activities must support compliance with:

- Australian laws and regulations;
- ACFID Code of Conduct obligations;
- Safeguarding standards;
- Financial integrity requirements;
- Privacy and confidentiality obligations;
- Relevant donor and funding conditions.

6.9 Respect for Human Rights and Dignity

BCDC recognises that effective risk management must uphold:

- Human dignity;
- Equality;
- Inclusion;
- Cultural respect;
- Non-discrimination;
- Community empowerment.

Risk management measures should avoid causing unnecessary harm, exclusion, stigma, or inequitable impacts on affected individuals or communities.

7. Legal and Regulatory Framework

BCDC is committed to ensuring that its risk management systems, governance practices, safeguarding mechanisms, and operational procedures align with relevant legal, regulatory, ethical, and sector standards applicable to its work in Australia and international operational contexts.

This Risk Management Policy is informed by, and intended to support compliance with, the following frameworks and obligations.

7.1 Australian Charities and Not-for-profits Commission (ACNC)

BCDC recognises its obligations under the Australian Charities and Not-for-profits Commission (ACNC), including:

- Governance Standards;
- External Conduct Standards;
- Financial accountability requirements;
- Responsible management obligations.

The organisation is committed to maintaining effective governance and operational systems that support lawful, ethical, and accountable activities.

7.2 ACFID Code of Conduct

This policy supports BCDC's commitment to complying with the Australian Council for International Development (ACFID) Code of Conduct, including obligations relating to:

- Safeguarding;
- Governance;
- Risk management;
- Financial integrity;
- Partnerships;
- Transparency;
- Accountability;
- Prevention of sexual exploitation, abuse, and harassment;
- Child protection;
- Counter-terrorism compliance.

7.3 Australian Laws and Regulatory Obligations

BCDC seeks to comply with all relevant Australian laws and regulatory requirements applicable to its activities, including obligations relating to:

- Workplace health and safety;
- Anti-discrimination;
- Privacy and confidentiality;
- Employment and volunteer management;
- Financial management and fraud prevention;
- Child protection and safeguarding;
- Recordkeeping and reporting obligations.

7.4 Counter-Terrorism and Sanctions Compliance

BCDC acknowledges obligations relating to:

- Australian counter-terrorism legislation;
- Sanctions compliance requirements;
- DFAT sanctions obligations;
- Prevention of financing prohibited entities.

The organisation may conduct reasonable due diligence and sanctions screening processes when engaging:

- Partners;
- Suppliers;
- Funding recipients;
- Contractors;
- Collaborating entities.

7.5 Privacy and Confidentiality Obligations

BCDC recognises the importance of protecting personal, confidential, safeguarding-related, and sensitive information.

The organisation seeks to maintain systems and procedures that support:

- Secure information management;
- Appropriate consent processes;
- Confidential handling of records;
- Protection against unauthorised disclosure or misuse of information.

7.6 Safeguarding and Protection Standards

This policy aligns with BCDC's safeguarding obligations and associated organisational policies, including:

- Child Safeguarding Policy;
- PSEAH Policy;
- Complaint Handling Policy;
- Human Resources Management Policy;
- Code of Conduct;
- Volunteer Manual.

BCDC is committed to maintaining safe and respectful environments free from exploitation, abuse, neglect, harassment, discrimination, and violence.

7.7 Humanitarian and Development Good Practice Principles

BCDC recognises internationally accepted principles relating to:

- Human rights;
- Human dignity;
- Inclusion and participation;
- Accountability to affected populations;
- Ethical humanitarian practice;
- Conflict sensitivity;
- Do No Harm approaches.

These principles inform BCDC's risk management practices across humanitarian, development, and community-based activities.

7.8 Organisational Policies and Internal Procedures

This Risk Management Policy should be read together with all relevant BCDC governance, safeguarding, operational, financial, and accountability policies and procedures.

Internal organisational systems, operational guidelines, and risk management tools may be developed to support implementation of this policy and compliance with relevant obligations.

8. Alignment with ACFID Code of Conduct

The Burmese Community Development Collaboration (BCDC) is committed to upholding the principles, obligations, and good practice standards outlined in the Australian Council for International Development (ACFID) Code of Conduct.

BCDC recognises that effective risk management is an essential component of accountable governance, safeguarding, ethical operational practice, financial integrity, and responsible humanitarian and development programming. This Risk Management Policy therefore supports BCDC's broader organisational commitment to implementing and maintaining systems that align with ACFID Code requirements and sector good practice standards.

This policy contributes to BCDC's compliance with ACFID Code obligations relating to:

- Governance and organisational oversight;
- Safeguarding and protection;
- Prevention of sexual exploitation, abuse, and harassment (PSEAH);
- Child safeguarding;
- Financial integrity and fraud prevention;
- Partnerships and due diligence;
- Risk management and operational accountability;
- Ethical fundraising and public communications;
- Complaints handling and whistleblower protections;
- Inclusion, accessibility, and protection of vulnerable individuals;
- Environmental sustainability and climate-conscious operations;
- Transparency and accountability to stakeholders.

BCDC recognises that risk management must not operate in isolation from safeguarding, financial management, accountability systems, and program quality. The organisation therefore seeks to integrate risk management principles into:

- Strategic planning and governance processes;
- Safeguarding systems and incident management;
- Program design and implementation;
- Human resources and volunteer management;
- Partnership selection and oversight;
- Monitoring, evaluation, accountability, and learning systems;
- Financial management and internal controls;
- Crisis preparedness and operational continuity planning.

BCDC further recognises that humanitarian and community-based organisations operating in complex environments must maintain heightened awareness of:

- Safeguarding vulnerabilities;
- Security threats;
- Fraud and corruption risks;
- Counter-terrorism obligations;
- Reputational risks;
- Risks associated with vulnerable and displaced populations.

Accordingly, BCDC commits to implementing reasonable and proportionate risk management systems that support:

- Prevention and early identification of risks;
- Safe and ethical operational practices;
- Continuous organisational learning and improvement;
- Protection of affected individuals and communities;
- Transparent and accountable decision-making;
- Responsible stewardship of resources and donor funds.

This policy also supports BCDC's commitment to maintaining a culture in which:

- Concerns and incidents can be reported safely and confidentially;
- Risks are openly discussed and appropriately escalated;
- Safeguarding and ethical responsibilities are prioritised;
- Organisational learning is encouraged;
- Accountability mechanisms are accessible and effective.

BCDC acknowledges that compliance with the ACFID Code of Conduct is an ongoing process requiring regular review, strengthening of systems, and adaptation to emerging operational risks and sector expectations. The organisation is therefore committed to continuously improving its governance, safeguarding, accountability, and risk management frameworks in alignment with evolving ACFID guidance and sector best practice.

9. Governance and Oversight Responsibilities

BCDC recognises that effective risk management requires strong governance, clear accountability structures, defined responsibilities, and active organisational oversight at all levels of the organisation.

Risk management is considered a shared responsibility across BCDC's governance structures, leadership, staff, volunteers, and partner organisations. All individuals associated with BCDC are expected to contribute to identifying, reporting, managing, and mitigating risks within their respective areas of responsibility.

9.1 Board Responsibilities

The BCDC Board holds overall responsibility for organisational governance and oversight of risk management systems.

The Board is responsible for:

- Providing strategic oversight of organisational risks;
- Promoting a culture of accountability, safeguarding, transparency, and ethical conduct;
- Ensuring that appropriate risk management systems, frameworks, and controls are established and maintained;
- Reviewing significant organisational risks and mitigation strategies;
- Monitoring high-risk operational activities and safeguarding concerns;
- Ensuring compliance with legal, regulatory, safeguarding, and ACFID obligations;
- Supporting financial integrity and responsible stewardship of organisational resources;
- Reviewing serious incidents, complaints, fraud concerns, safeguarding reports, or operational crises where appropriate;
- Ensuring that adequate resources are allocated to support risk management and safeguarding systems;
- Supporting organisational resilience and continuity planning.

The Board may delegate specific operational risk management functions to management personnel while retaining overall governance oversight responsibilities.

9.2 Executive and Management Responsibilities

Executive leadership and management personnel are responsible for implementing and operationalising BCDC's risk management systems and procedures.

Management responsibilities include:

- Implementing this Risk Management Policy across organisational operations;
- Maintaining and monitoring the organisational Risk Register;
- Conducting risk assessments and coordinating mitigation measures;
- Supporting safe operational practices and safeguarding systems;
- Ensuring that staff and volunteers receive relevant training and guidance;
- Monitoring operational, financial, safeguarding, and partnership risks;
- Responding appropriately to incidents, complaints, and emerging risks;
- Escalating significant risks or incidents to the Board where required;
- Supporting compliance with legal, financial, safeguarding, and reporting obligations;
- Monitoring organisational preparedness for emergencies and operational disruptions.

Management is also responsible for ensuring that risk management considerations are integrated into:

- Program planning;
- Budgeting and procurement;
- Recruitment and onboarding;
- Partnership engagement;
- Monitoring and evaluation processes;
- Operational decision-making.

9.3 Staff Responsibilities

All staff members are responsible for contributing to a safe, ethical, accountable, and risk-aware organisational environment.

Staff responsibilities include:

- Complying with this policy and associated organisational procedures;
- Identifying and reporting risks, incidents, concerns, or operational issues promptly;
- Following safeguarding, financial, operational, and security procedures;
- Participating in training and organisational risk management processes;
- Supporting safe and respectful operational practices;
- Maintaining confidentiality and protecting organisational information;
- Cooperating with investigations, reviews, and corrective actions where required.

Staff members are expected to exercise reasonable judgment and take practical steps to minimise risks within their areas of work.

9.4 Volunteer Responsibilities

Volunteers, interns, and community representatives engaged by BCDC are expected to:

- Follow organisational policies and procedures;
- Participate in safeguarding and safety practices;
- Report concerns, incidents, or emerging risks promptly;
- Support respectful, safe, and ethical interactions with communities and stakeholders;
- Contribute to maintaining safe operational environments.

Volunteers are expected to seek guidance from supervisors where uncertain about risk-related matters or operational concerns.

9.5 Partner Organisation Responsibilities

Partner organisations and collaborating entities involved in BCDC-supported activities are expected to:

- Operate in a manner consistent with safeguarding and ethical standards;
- Participate in due diligence and risk assessment processes;
- Cooperate with monitoring, reporting, and accountability mechanisms;
- Take reasonable steps to identify and manage operational risks;
- Notify BCDC of significant incidents, safeguarding concerns, fraud allegations, or security issues that may affect joint activities.

BCDC may apply proportionate oversight and monitoring measures depending on:

- The level of partnership risk;
- Operational context;
- Nature of activities;
- Funding arrangements.

9.6 Shared Organisational Responsibility

BCDC recognises that effective risk management depends on collective organisational commitment and communication.

All individuals associated with BCDC are encouraged to:

- Raise concerns openly and responsibly;
- Participate in prevention-focused approaches;
- Support continuous improvement and organisational learning;
- Contribute to maintaining a culture of accountability, safeguarding, and ethical conduct.

The organisation is committed to ensuring that individuals who report concerns or risks in good faith are protected from retaliation, intimidation, or adverse treatment.

10. Risk Management Framework

BCDC adopts an organisation-wide and systematic approach to risk management designed to support good governance, safeguarding, operational effectiveness, legal compliance, financial integrity, and organisational sustainability.

The Risk Management Framework provides the structure through which risks are identified, assessed, managed, monitored, documented, and reviewed across all areas of organisational activity.

The framework is intended to:

- Promote consistent risk management practices across the organisation;
- Support informed and accountable decision-making;
- Strengthen organisational resilience and preparedness;
- Protect individuals, communities, organisational assets, and stakeholder trust;
- Support compliance with safeguarding, financial, legal, and governance obligations;
- Integrate risk management into strategic and operational planning processes.

BCDC's Risk Management Framework is based on the principle that risk management should be:

- Ongoing and proactive;
- Integrated into everyday organisational activities;
- Proportionate to the level and nature of risks;
- Context-sensitive and adaptable;
- Aligned with safeguarding and accountability principles;
- Supported by clear documentation and oversight mechanisms.

The framework includes:

- Risk identification processes;
- Risk assessment and rating systems;
- Organisational Risk Register;
- Risk mitigation and treatment measures;
- Incident reporting and escalation procedures;
- Monitoring and review mechanisms;
- Due diligence and partner screening processes;
- Safeguarding and protection integration;
- Crisis and emergency management procedures;
- Organisational learning and continuous improvement systems.

BCDC recognises that risks may evolve over time due to:

- Humanitarian emergencies;
- Conflict and political instability;
- Organisational growth;
- Partnership arrangements;
- Funding changes;
- Technological developments;
- Changes in legal or regulatory environments.

Accordingly, the organisation commits to regularly reviewing and strengthening its risk management systems to ensure that they remain effective, responsive, and appropriate to operational realities.

11. Risk Management Process

BCDC follows a structured and continuous process for identifying, assessing, managing, monitoring, and reviewing risks across all organisational activities.
The organisation recognises that risk management is not a one-time exercise, but an ongoing process integrated into governance, operations, safeguarding, partnerships, financial management, and program implementation.

11.1 Risk Identification

BCDC seeks to identify risks proactively and systematically before they result in harm, disruption, financial loss, safeguarding failures, or operational challenges.
Risks may be identified through:

- Strategic planning processes;
- Program design and implementation;
- Staff meetings and operational discussions;
- Community and stakeholder feedback;
- Incident and complaint reporting;
- Monitoring and evaluation activities;
- Financial oversight and audits;
- Safeguarding assessments;
- Partner due diligence processes;
- Travel and security assessments;
- External environmental or political developments.

Identified risks may relate to:

- Safeguarding;
- Financial integrity;
- Security;
- Legal compliance;
- Reputation;
- Partnerships;
- Operational continuity;
- Cybersecurity;
- Health and safety;
- Environmental sustainability.

11.2 Risk Assessment

Once identified, risks are assessed to determine:

- The likelihood of occurrence;
- The potential severity of consequences;
- The level of organisational exposure;
- The vulnerability of affected individuals or systems.

Risk assessments consider:

- Existing controls and safeguards;
- Operational context;
- Humanitarian or conflict-related conditions;
- Safeguarding implications;
- Resource limitations;
- Potential impacts on stakeholders and communities.

11.3 Risk Analysis

BCDC analyses identified risks to understand:

- Root causes;
- Contributing factors;
- Potential consequences;
- Interconnections between risks;
- Areas requiring priority attention.

This analysis supports informed decision-making and prioritisation of mitigation measures.

11.4 Risk Rating and Prioritisation

Risks are categorised and prioritised according to their assessed:

- Likelihood; and
- Impact.

Risk ratings may include:

- Low Risk;
- Moderate Risk;
- High Risk;
- Critical Risk.

Higher-risk issues may require:

- Immediate mitigation measures;
- Increased oversight;
- Escalation to management or Board level;
- Additional monitoring and reporting requirements.

11.5 Risk Treatment and Mitigation

BCDC implements reasonable and proportionate measures to reduce identified risks wherever possible.

Mitigation measures may include:

- Safeguarding controls;
- Financial controls;
- Staff training;
- Policy development;
- Supervision and oversight;
- Due diligence procedures;
- Incident response mechanisms;
- Security protocols;
- Operational adjustments;
- Monitoring systems.

Where risks cannot be fully eliminated, BCDC seeks to reduce residual risks to acceptable levels.

11.6 Monitoring and Review

Risks, mitigation measures, and operational conditions are monitored regularly to ensure that:

- Controls remain effective;
- Emerging risks are identified;
- Risk levels remain appropriate;
- Lessons learned inform organisational improvement.

Monitoring activities may include:

- Internal reviews;
- Risk Register updates;
- Incident trend analysis;
- Staff and stakeholder feedback;
- Program monitoring processes;
- Safeguarding reviews;
- Governance oversight meetings.

11.7 Reporting and Escalation

All personnel are expected to report:

- Significant risks;
- Emerging threats;
- Safeguarding concerns;
- Fraud allegations;
- Operational incidents;
- Security issues;
- Serious misconduct.

BCDC maintains reporting and escalation mechanisms designed to support:

- Timely response;
- Confidentiality;
- Accountability;
- Appropriate oversight;
- Organisational learning.

Serious or high-risk matters may be escalated to senior management, the Board, external authorities, or relevant regulators where appropriate.

12. Categories of Organisational Risks

BCDC recognises that risks may arise across all organisational operations, governance functions, partnerships, humanitarian activities, safeguarding systems, financial management processes, and service delivery activities. The organisation therefore adopts a broad and integrated approach to identifying and managing organisational risks.
The categories below are intended to support systematic identification, assessment, monitoring, and mitigation of risks across all levels of organisational activity.

12.1 Safeguarding Risks

Safeguarding risks include any risk that may result in harm, abuse, exploitation, neglect, harassment, discrimination, violence, or unsafe practices affecting children, vulnerable adults, beneficiaries, communities, staff, volunteers, or stakeholders.
These may include:

- Child abuse or neglect;
- Sexual exploitation, abuse, or harassment;
- Unsafe recruitment or supervision;
- Failure to respond appropriately to safeguarding concerns;
- Breaches of confidentiality relating to safeguarding matters.

12.2 Child Protection Risks

BCDC recognises that children involved in, affected by, or exposed to organisational activities may face heightened vulnerabilities.
Child protection risks may include:

- Unsafe interactions with children;
- Inadequate screening of personnel;
- Exposure to harmful environments;
- Inappropriate communication or imagery involving children;
- Failure to report child safeguarding concerns.

12.3 PSEAH Risks

Risks relating to sexual exploitation, abuse, and harassment (SEAH) may arise in organisational, humanitarian, community-based, and partnership settings.
BCDC recognises the importance of maintaining:

- Survivor-centred approaches;
- Confidential reporting systems;
- Prevention-focused safeguarding mechanisms;
- Appropriate investigation and response procedures.

12.4 Financial Risks

Financial risks include risks that may negatively affect:

- Organisational sustainability;
- Financial accountability;
- Resource management;
- Donor confidence.

Examples may include:

- Budget shortfalls;
- Weak internal controls;
- Inaccurate reporting;
- Financial mismanagement;
- Cash flow challenges.

12.5 Fraud and Corruption Risks

Fraud and corruption risks include:

- Theft;
- Bribery;
- Embezzlement;
- Misuse of funds;
- Financial misconduct;
- Procurement manipulation;
- Corrupt practices;
- Unauthorised financial transactions.

12.6 Operational Risks

Operational risks refer to risks that may disrupt organisational activities, programs, systems, or services.

Examples include:

- Inadequate procedures;
- Communication failures;
- Staffing shortages;
- Poor coordination;
- Program implementation delays;
- Technology failures.

12.7 Human Resource Risks

Human resource risks may include:

- Unsafe workplace conditions;
- Inadequate supervision;
- Workplace conflict;
- Staff burnout;
- Inadequate training;
- High staff turnover;
- Recruitment and retention challenges.

12.8 Volunteer Management Risks

Volunteer-related risks may include:

- Insufficient induction;
- Inadequate supervision;
- Unclear responsibilities;
- Safeguarding concerns;
- Health and safety risks;
- Role misunderstandings.

12.9 Health and Safety Risks

BCDC recognises the importance of maintaining safe and healthy working environments.

Health and safety risks may include:

- Workplace injuries;
- Unsafe facilities;
- Exposure to hazardous conditions;
- Psychological stress;
- Travel-related safety concerns.

12.10 Security Risks

Security risks may arise from:

- Conflict and political instability;
- Community tensions;
- Threats to personnel;
- Violence;
- Theft;
- Unstable operational environments.

12.11 Overseas Travel Risks

Travel-related risks may include:

- Conflict exposure;
- Border restrictions;
- Limited medical access;
- Communication breakdowns;
- Security incidents;
- Travel disruptions.

12.12 Myanmar and Border Area Risks

BCDC recognises that operations involving Myanmar and border regions may involve elevated risks due to:

- Armed conflict;
- Political instability;
- Humanitarian crises;
- Security restrictions;
- Limited infrastructure;
- Displacement and vulnerability.

12.13 Partnership and Due Diligence Risks

Partnership risks may include:

- Weak governance structures;
- Safeguarding failures;
- Financial misconduct;
- Reputational concerns;
- Misalignment with organisational values;
- Counter-terrorism or sanctions concerns.

12.14 Legal and Compliance Risks

Legal and compliance risks include risks associated with:

- Breach of laws or regulations;
- Non-compliance with ACFID obligations;
- Regulatory penalties;
- Failure to meet reporting obligations.

12.15 Privacy and Data Protection Risks

Privacy risks may include:

- Data breaches;
- Unauthorised disclosure;
- Loss of confidential information;
- Improper handling of personal data.

12.16 Cybersecurity and Information Risks

Cybersecurity risks may include:

- Hacking;
- Malware;
- Unauthorised access;
- Loss of digital records;
- Information system failures.

12.17 Reputational Risks

Reputational risks may arise from:

- Misconduct allegations;
- Safeguarding failures;
- Public complaints;
- Inaccurate public communications;
- Operational failures;
- Ethical concerns.

12.18 Environmental and Climate Risks

Environmental risks may include:

- Natural disasters;
- Climate-related disruptions;
- Environmental harm caused by operations;
- Reduced access due to extreme weather conditions.

12.19 Community Relations Risks

Community-related risks may include:

- Loss of trust;
- Community dissatisfaction;
- Cultural misunderstandings;
- Exclusion or discrimination concerns;
- Inadequate consultation processes.

12.20 Program Delivery Risks

Program delivery risks may include:

- Delays in implementation;
- Inadequate resources;
- Failure to achieve intended outcomes;
- Weak monitoring systems;
- Inconsistent service quality.

13. Risk Assessment Matrix and Risk Rating System

BCDC applies a structured risk assessment and rating system to support consistent evaluation and prioritisation of organisational risks.
Risk assessments are conducted to:

- Determine the seriousness of risks;
- Support informed decision-making;
- Identify appropriate mitigation measures;
- Allocate organisational oversight and resources proportionately.

13.1 Risk Assessment Criteria

Risks are assessed based on:

- Likelihood of occurrence; and
- Potential impact or consequences.

13.2 Likelihood Ratings

Likelihood refers to the probability that a risk may occur.

Rating	Description
Rare	Unlikely to occur except in exceptional circumstances
Unlikely	Could occur occasionally
Possible	May occur under certain circumstances
Likely	Expected to occur in many circumstances
Almost Certain	Expected to occur frequently or repeatedly

13.3 Impact Ratings

Impact refers to the severity of consequences if the risk occurs.

Rating	Description
Minor	Limited impact with manageable consequences
Moderate	Noticeable operational or reputational impact
Significant	Serious disruption, harm, or financial impact
Major	Severe organisational, safeguarding, or legal consequences
Critical	Extreme harm, major operational failure, or significant legal/reputational damage

13.4 Risk Rating Categories

Risk ratings may be categorised as:

- Low Risk;
- Moderate Risk;
- High Risk;
- Critical Risk.

Higher-risk matters may require:

- Immediate mitigation measures;
- Increased oversight;
- Escalation to management or Board level;
- Additional monitoring and controls.

14. Risk Register

BCDC will maintain an organisational Risk Register to document and monitor identified risks across all operational areas.

The Risk Register may include:

- Description of risks;
- Risk categories;
- Likelihood and impact ratings;
- Existing controls;
- Mitigation measures;
- Responsible personnel;
- Review dates;
- Status updates.

The Risk Register supports:

- Organisational oversight;
- Accountability;
- Monitoring and review;
- Strategic planning;
- Operational decision-making.

The Risk Register will be reviewed periodically by management and, where appropriate, by the Board.

15. High-Risk Activities and Approval Procedures

BCDC recognises that certain activities may involve elevated risks requiring additional oversight, planning, approval, and mitigation measures.

Examples of high-risk activities may include:

- Travel to conflict-affected areas;
- Cross-border operations;
- Humanitarian emergency response;
- Activities involving vulnerable populations;
- Large public events;
- Activities involving financial transfers or procurement in unstable environments.

Prior to approving high-risk activities, BCDC may conduct:

- Risk assessments;
- Safeguarding reviews;
- Security assessments;
- Operational planning reviews;
- Due diligence checks.

Approval requirements may vary depending on:

- Risk level;
- Operational context;
- Nature of activities;
- Potential safeguarding implications.

BCDC reserves the right to postpone, modify, restrict, or decline activities where risks are considered unacceptable.

16. Overseas Travel Risk Management Procedures

BCDC recognises that overseas travel may involve heightened security, safeguarding, legal, logistical, and health-related risks.

Prior to approving overseas travel, BCDC may consider:

- DFAT travel advisories;
- Security conditions;
- Local partner advice;
- Medical access;
- Communication systems;
- Safeguarding considerations;
- Insurance availability;
- Operational necessity.

Travellers may be required to:

- Participate in safety briefings;
- Follow emergency communication procedures;
- Comply with safeguarding obligations;
- Report incidents promptly.

Where risks are considered unacceptable, travel may be restricted, postponed, or not approved.

17. Incident Reporting and Escalation Procedures

BCDC maintains procedures for reporting and responding to:

- Safeguarding concerns;
- Fraud allegations;
- Security incidents;
- Workplace incidents;
- Serious misconduct;
- Operational risks.

All personnel are expected to report significant incidents or concerns promptly through appropriate organisational channels.

Reports may be escalated to:

- Management;
- Safeguarding focal persons;
- Board representatives;
- External authorities where legally required.

BCDC seeks to maintain reporting systems that are:

- Confidential;
- Accessible;
- Fair;
- Survivor-centred where applicable;
- Free from retaliation.

18. Crisis and Emergency Management

BCDC recognises that emergencies and crises may significantly disrupt operations and affect the safety and wellbeing of stakeholders.

Possible emergencies may include:

- Security incidents;
- Conflict escalation;
- Natural disasters;
- Cybersecurity incidents;
- Safeguarding emergencies;
- Public health emergencies.

BCDC may implement:

- Emergency response procedures;
- Crisis communication measures;
- Temporary operational adjustments;
- Evacuation or relocation measures;
- Incident coordination systems.

19. Fraud Prevention and Financial Control Measures

BCDC is committed to maintaining strong financial integrity and accountability systems. Fraud prevention measures may include:

- Segregation of duties;
- Financial oversight and approvals;
- Budget monitoring;
- Procurement controls;
- Financial reporting;
- Audits and reviews;
- Whistleblower protections;
- Due diligence procedures.

Suspected financial wrongdoing must be reported promptly and managed in accordance with relevant organisational policies.

20. Due Diligence and Sanctions Screening

BCDC conducts proportionate due diligence processes before entering into:

- Partnerships;
- Funding arrangements;
- Procurement engagements;
- Operational collaborations.

Due diligence processes may include:

- Governance assessments;
- Safeguarding reviews;
- Financial integrity checks;
- Reference checks;
- Public information reviews;
- Screening against sanctions and prohibited entities lists.

BCDC may conduct reasonable checks against relevant Australian Government and DFAT sanctions databases where appropriate.

21. Safeguarding and Risk Integration

BCDC recognises that safeguarding considerations must be integrated into all organisational risk management processes.

Risk management activities should consider:

- Child safeguarding risks;
- PSEAH risks;
- Vulnerabilities affecting communities and individuals;
- Power imbalances;
- Accessibility and inclusion concerns.

Safeguarding considerations must be integrated into:

- Program design;
- Recruitment;
- Partnerships;
- Travel planning;
- Community engagement;
- Incident response processes.

22. Business Continuity and Operational Continuity

BCDC seeks to maintain operational continuity during periods of disruption or crisis.
Business continuity planning may include:

- Alternative communication arrangements;
- Remote operational systems;
- Data backup procedures;
- Delegation of responsibilities;
- Emergency coordination arrangements;
- Operational contingency planning.

The organisation recognises the importance of maintaining critical services and safeguarding obligations during emergencies or disruptions.

23. Documentation and Record Keeping

BCDC will maintain appropriate documentation relating to:

- Risk assessments;
- Incident reports;
- Risk Registers;
- Mitigation measures;
- Investigations;
- Monitoring and review activities.

Records should be:

- Accurate;
- Secure;
- Confidential where appropriate;
- Accessible to authorised personnel only.

24. Training and Capacity Building

BCDC is committed to strengthening organisational understanding and capacity relating to risk management.

Training and awareness activities may include:

- Safeguarding training;
- Fraud prevention awareness;
- Incident reporting procedures;
- Security awareness;
- Risk assessment processes;
- Emergency response procedures.

Training may be provided to:

- Board members;
- Staff;
- Volunteers;
- Partner organisations.

25. Monitoring, Evaluation, and Continuous Improvement

BCDC recognises that risk management systems require ongoing monitoring, learning, and improvement.

The organisation may review:

- Incident trends;
- Operational risks;
- Mitigation effectiveness;
- Stakeholder feedback;
- Audit findings;
- Lessons learned from emergencies or incidents.

Findings may inform:

- Policy revisions;
- Training improvements;
- Operational changes;
- Strengthening of controls and safeguards.

26. Policy Breaches and Non-Compliance

Failure to comply with this policy or associated procedures may result in:

- Disciplinary action;
- Suspension of responsibilities;
- Termination of employment or engagement;
- Partnership review or termination;
- Referral to relevant authorities where required.

BCDC may investigate allegations of non-compliance in accordance with organisational procedures.

27. Confidentiality and Protection of Information

BCDC recognises the importance of protecting confidential, personal, safeguarding-related, and organisational information.

All personnel are expected to:

- Maintain confidentiality;
- Protect sensitive information;
- Prevent unauthorised disclosure;
- Follow organisational privacy procedures.

Confidential information should only be shared on a need-to-know basis or where legally required.

28. Review and Policy Update Process

This policy will be reviewed periodically to ensure ongoing relevance, effectiveness, and alignment with:

- Operational contexts;
- Legal obligations;
- ACFID requirements;
- Organisational learning;
- Emerging risks and sector standards.

The policy may also be reviewed following:

- Serious incidents;
- Safeguarding concerns;
- Operational crises;
- Significant organisational changes.

29. Related Policies and Supporting Documents

This policy should be read together with:

- Child Safeguarding Policy;
- PSEAH Policy;
- Complaint Handling Policy;
- Financial Wrongdoing Policy;
- PMEL Policy;
- Partnership Commitment Policy;
- Privacy Policy;
- Human Resources Management Policy;
- Volunteer Manual;
- Code of Conduct;
- Non-Development Activity Policy;
- Environmental Sustainability and Climate Action Policy;
- Due Diligence Procedures;
- Risk Register Templates;
- Incident Reporting Forms;
- Emergency Procedures.

30.Appendices

Appendix A – Risk Rating Matrix
Appendix B – Organisational Risk Register Template
Appendix C – Incident Reporting Flow
Appendix D – Travel Risk Assessment Template
Appendix E – Due Diligence Checklist
Appendix F – Emergency Contact Procedures
Appendix G – Partner Risk Screening Checklist
Appendix H – Safeguarding Risk Assessment Guide
Appendix I – Risk Monitoring and Review Schedule

Appendix A – Risk Rating Matrix

Burmese Community Development Collaboration (BCDC)

Risk Rating Matrix

Purpose

This Risk Rating Matrix is used by the Burmese Community Development Collaboration (BCDC) to support consistent assessment, prioritisation, monitoring, and management of organisational risks across all operational, safeguarding, financial, governance, partnership, and programmatic activities.

The matrix assists BCDC personnel in:

- Assessing the seriousness of identified risks;
- Determining appropriate mitigation measures;
- Supporting informed decision-making;
- Prioritising organisational attention and resources;
- Escalating high-risk matters appropriately.

This matrix should be used together with:

- Risk assessments;
- Risk Registers;
- Incident reporting procedures;
- Safeguarding assessments;
- Operational planning processes.

A. Likelihood Rating Scale

Likelihood refers to the probability or frequency that a risk may occur.

Likelihood Level		Description	Example Indicators
1	Rare	May occur only in exceptional circumstances	No previous incidents; highly unlikely situation
2	Unlikely	Could occur occasionally but not expected regularly	Limited history of occurrence
3	Possible	May occur under certain circumstances	Could reasonably happen during operations
4	Likely	Expected to occur in many circumstances	Repeated operational concerns or recurring vulnerabilities
5	Almost Certain	Expected to occur frequently or repeatedly	Ongoing or highly predictable risk exposure

B. Impact Rating Scale

Impact refers to the severity of consequences if the risk occurs.

Rating	Impact Level	Description	Example Consequences
1	Minor	Limited impact with manageable consequences	Small operational disruption; minimal reputational effect
2	Moderate	Noticeable impact requiring management attention	Temporary service disruption; manageable financial loss
3	Significant	Serious operational, safeguarding, or financial consequences	Program interruption; safeguarding concern; reputational impact
4	Major	Severe organisational or legal consequences	Major safeguarding breach; significant financial loss; legal implications
5	Critical	Extreme harm or organisational crisis	Serious injury/death; large-scale fraud; major reputational collapse; operational shutdown

C. Risk Rating Matrix

The overall risk rating is determined by combining:

- Likelihood score; and
- Impact score.

Likelihood \ Impact	1 Minor	2 Moderate	3 Significant	4 Major	5 Critical
5 Almost Certain	Moderate	High	High	Critical	Critical
4 Likely	Moderate	Moderate	High	High	Critical
3 Possible	Low	Moderate	Moderate	High	Critical
2 Unlikely	Low	Low	Moderate	High	High
1 Rare	Low	Low	Moderate	Moderate	High

D. Risk Rating Categories and Required Responses

Low Risk

Description

- Acceptable and manageable risk level.
- Minimal operational or safeguarding impact expected.

Required Actions

- Monitor periodically.
- Maintain existing controls.
- Record in Risk Register where appropriate.

Moderate Risk

Description

- Noticeable risk requiring active management and monitoring.
- May affect operations, safeguarding, finances, or reputation if unmanaged.

Required Actions

- Implement mitigation measures.
- Assign responsible personnel.
- Review regularly.
- Monitor effectiveness of controls.

High Risk

Description

- Serious risk requiring immediate management attention.
- Significant potential impact on safeguarding, operations, finances, or reputation.

Required Actions

- Immediate mitigation planning required.
- Escalate to management.
- Increase monitoring and oversight.
- Review operational feasibility and controls.

Critical Risk

Description

- Extreme or unacceptable risk level.
- Potential for severe harm, legal consequences, organisational crisis, or operational failure.

Required Actions

- Immediate escalation to senior management and/or Board.
- Consider suspension, postponement, or cancellation of activities.

- Implement urgent risk treatment measures.
- Develop emergency response actions.
- Monitor continuously.

E. Risk Assessment Guidance

When assessing risks, personnel should consider:

- Vulnerability of affected individuals;
- Safeguarding implications;
- Security and conflict conditions;
- Financial exposure;
- Operational capacity;
- Legal and compliance obligations;
- Reputational impact;
- Likelihood of escalation or recurrence.

Assessments should also consider:

- Existing controls and safeguards;
- Local operational context;
- Humanitarian and conflict-related conditions;
- Partner capacity and reliability;
- Community feedback and stakeholder concerns.

F. Examples of Risks That May Require High or Critical Ratings

Examples may include:

- Serious safeguarding allegations;
- Sexual exploitation or abuse concerns;
- Fraud or corruption allegations;
- Travel to active conflict zones;
- Major cybersecurity breaches;
- Serious legal non-compliance;
- Significant financial losses;
- Threats to staff safety;

- Partnership with prohibited entities;
- Large-scale operational disruptions.

G. Review and Updating of Risk Ratings

Risk ratings should be reviewed:

- During regular operational reviews;
- Following incidents or emergencies;
- When operational contexts change;
- When new risks emerge;
- During program planning and implementation;
- During monitoring and evaluation activities.

Risk levels may increase or decrease depending on:

- Effectiveness of mitigation measures;
- Changes in operational conditions;
- Organisational capacity;
- External environmental factors.

H. Integration with Organisational Systems

This Risk Rating Matrix should be used together with:

- Risk Registers;
- Safeguarding assessments;
- Incident reporting systems;
- Due diligence procedures;
- Emergency management processes;
- Monitoring and evaluation systems;
- Financial oversight mechanisms.

The matrix forms part of BCDC's broader organisational risk management framework and supports compliance with safeguarding, governance, financial accountability, and ACFID Code obligations.

Appendix B – Organisational Risk Register Template

Burmese Community Development Collaboration (BCDC)

Organisational Risk Register Template

Purpose

This Organisational Risk Register Template is designed to support the systematic identification, assessment, monitoring, mitigation, management, and review of risks across all BCDC governance, safeguarding, operational, financial, partnership, humanitarian, and programmatic activities.

The Risk Register assists BCDC in:

- Identifying organisational vulnerabilities and operational threats;
- Recording and monitoring risks consistently;
- Supporting informed governance and operational decision-making;
- Strengthening safeguarding, accountability, and compliance systems;
- Prioritising mitigation and control measures;
- Supporting organisational resilience and continuity planning;
- Demonstrating compliance with ACFID, safeguarding, and governance obligations.

This register should be reviewed regularly and updated whenever:

- New risks emerge;
- Operational contexts change;
- Serious incidents occur;

- Programs expand or change;
- New partnerships are established;
- Safeguarding or financial concerns arise;
- External humanitarian, political, or security conditions shift.

Risk Rating Reference

Risk Rating	Description	Required Response
Low	Acceptable and manageable risk	Monitor periodically
Moderate	Requires active management	Implement mitigation measures and review regularly
High	Significant risk requiring urgent attention	Escalate to management and strengthen controls
Critical	Extreme or unacceptable risk	Immediate escalation and urgent response required

Organisational Risk Register Table

Risk ID	Risk Category	Description of Risk	Potential Impact	Existing Controls	Likelihood	Impact	Overall Risk Rating	Mitigation Actions Required	Responsible Person	Review Frequency	Status / Comments
BCDC-R001	Safeguarding Risk	Risk of harm, abuse, or exploitation of vulnerable beneficiaries during activities	Harm to individuals, safeguarding breach, reputational damage	Safeguarding Policy, Code of Conduct, training	Possible	Major	High	Strengthen supervision and safeguarding monitoring	Safeguarding Focal Person	Quarterly	Ongoing
BCDC-R002	Child Protection Risk	Inappropriate interaction or unsafe engagement with children	Harm to children, legal consequences, reputational damage	Child Safeguarding Policy, WWCC screening, reporting procedures	Possible	Critical	Critical	Improve safeguarding induction and supervision	Safeguarding Team	Quarterly	Active Monitoring

BCDC-R003	PSEAH Risk	Sexual exploitation, abuse, or harassment involving staff, volunteers, or stakeholders	Serious harm, safeguarding breach, reputational impact	PSEAH Policy, reporting mechanisms, training	Possible	Critical	Critical	Strengthen awareness and confidential reporting pathways	Executive Team	Quarterly	Ongoing
BCDC-R004	Financial Risk	Mismanagement or misuse of organisational funds	Financial loss, donor concerns, operational disruption	Financial controls, approvals, audits	Unlikely	Major	High	Strengthen financial monitoring systems	Finance Officer	Quarterly	Under Review
BCDC-R005	Fraud and Corruption Risk	Fraudulent transactions, bribery, or misuse of resources	Financial loss, reputational harm, legal consequences	Segregation of duties, approval systems	Possible	Major	High	Conduct periodic financial reviews and training	Finance Officer	Quarterly	Ongoing
BCDC-R006	Operational Risk	Program delays or operational disruptions due to inadequate procedures	Reduced program effectiveness, stakeholder dissatisfaction	Operational planning and supervision	Possible	Significant	Moderate	Improve coordination and operational monitoring	Program Manager	Quarterly	In Progress
BCDC-R007	Human Resource Risk	Staff burnout, conflict, or inadequate staffing capacity	Reduced organisational effectiveness, staff wellbeing concerns	HR procedures, supervision, leave management	Likely	Moderate	Moderate	Improve staff wellbeing and support systems	HR Focal Person	Quarterly	Ongoing
BCDC-R008	Volunteer Risk	Volunteers may lack sufficient training or safeguarding awareness	Safeguarding concerns, operational inconsistency	Volunteer induction and Code of Conduct	Possible	Significant	Moderate	Strengthen volunteer orientation and supervision	Volunteer Coordinator	Quarterly	Ongoing
BCDC-R009	Health and Safety Risk	Workplace injury, illness, or unsafe operational environment	Physical harm, operational disruption	Safety procedures and reporting systems	Possible	Major	High	Conduct periodic workplace safety reviews	Management Team	Quarterly	Under Review
BCDC-R010	Security Risk	Security threats affecting personnel or operations in unstable environments	Injury, operational suspension, evacuation	Security planning and local coordination	Possible	Critical	Critical	Restrict high-risk travel and strengthen emergency preparedness	Executive Team	Monthly	Active Monitoring
BCDC-R011	Overseas Travel Risk	Staff or volunteers travelling to Myanmar or border areas may face security and logistical risks	Injury, detention, travel disruption, communication failure	Travel approvals and contextual risk assessments	Possible	Critical	Critical	Strengthen travel approval and monitoring procedures	Executive Team	Monthly	Active Monitoring
BCDC-R012	Myanmar and Border Area Risk	Conflict escalation and humanitarian instability affecting cross-border activities	Operational disruption, security threats, safeguarding risks	Context monitoring and local partner coordination	Likely	Critical	Critical	Ongoing contextual monitoring and contingency planning	Management Team	Monthly	Ongoing
BCDC-R013	Partnership and Due Diligence Risk	Partner organisations may have weak governance or safeguarding systems	Reputational damage, safeguarding concerns, compliance issues	Due diligence assessments and partner screening	Possible	Significant	High	Strengthen partner monitoring and due diligence	Program Manager	Quarterly	Ongoing

BCDC-R014	Legal and Compliance Risk	Failure to comply with ACFID, ACNC, safeguarding, or legal obligations	Legal consequences, reputational damage, compliance breaches	Governance oversight and policy framework	Unlikely	Major	High	Conduct compliance reviews and policy updates	Board / Executive Team	Quarterly	Under Review
BCDC-R015	Privacy and Data Protection Risk	Loss or unauthorised disclosure of confidential information	Privacy breach, reputational damage, stakeholder harm	Password protection and restricted access	Possible	Significant	Moderate	Strengthen data protection and confidentiality systems	Administration Team	Quarterly	In Progress
BCDC-R016	Cybersecurity Risk	Cyberattack, malware, or unauthorised access to organisational systems	Operational disruption, data loss, confidentiality breach	Password systems and data backup procedures	Likely	Significant	High	Improve cybersecurity awareness and system protections	Administration Team	Quarterly	Ongoing
BCDC-R017	Reputational Risk	Negative publicity or public complaints affecting organisational trust	Loss of donor and community confidence	Complaint Handling Policy and public communication procedures	Possible	Major	High	Strengthen communication and accountability mechanisms	Executive Team	Quarterly	Ongoing
BCDC-R018	Environmental and Climate Risk	Natural disasters or environmental disruptions affecting activities	Program delays, operational disruption, community impact	Flexible operational planning	Possible	Significant	Moderate	Improve emergency preparedness and contingency planning	Program Team	Annually	Under Review
BCDC-R019	Community Relations Risk	Community dissatisfaction, exclusion concerns, or cultural misunderstandings	Reduced trust and stakeholder engagement	Community consultation and feedback systems	Possible	Moderate	Moderate	Strengthen inclusive participation and communication	Community Engagement Team	Quarterly	Ongoing
BCDC-R020	Program Delivery Risk	Failure to achieve intended project outcomes or deliver services effectively	Reduced program effectiveness and donor confidence	PMEL systems and operational oversight	Possible	Significant	Moderate	Improve monitoring and adaptive management systems	Program Manager	Quarterly	Ongoing

Additional Risk Management Guidance

Review Process

The Risk Register should be:

- Reviewed regularly by management;
- Updated following incidents or operational changes;
- Discussed during governance and operational meetings;

- Escalated to the Board where significant risks are identified.

High-risk and critical-risk issues may require:

- Immediate mitigation actions;
- Increased monitoring;
- Emergency response measures;
- Temporary operational adjustments.

Confidentiality and Access

Risk Registers may contain sensitive organisational, safeguarding, financial, security, or operational information.

Accordingly:

- Access should be limited to authorised personnel;
- Safeguarding and security risks should be managed confidentially;
- Records should be stored securely and protected from unauthorised disclosure.

Integration with Organisational Systems

This Risk Register should be used together with:

- Risk Management Policy;
- Child Safeguarding Policy;
- PSEAH Policy;
- Financial Wrongdoing Policy;

- Complaint Handling Policy;
- PMEL systems;
- Due Diligence procedures;
- Incident reporting mechanisms;
- Emergency response procedures.

The register forms part of BCDC's broader governance, safeguarding, accountability, compliance, and organisational resilience framework.

Appendix C – Incident Reporting Flow

Burmese Community Development Collaboration (BCDC)

Incident Reporting and Escalation Flow

Purpose

This Incident Reporting Flowchart provides guidance for BCDC Board members, staff, volunteers, contractors, consultants, and partner organisations on the process for identifying, reporting, responding to, documenting, and escalating incidents, concerns, allegations, or operational risks.

The flowchart is intended to support:

- Timely and appropriate incident response;
- Safeguarding and protection obligations;
- Organisational accountability;
- Risk mitigation and operational oversight;
- Confidentiality and survivor-centred approaches;
- Compliance with BCDC policies and ACFID obligations.

This flowchart should be read together with:

- Risk Management Policy;
- Child Safeguarding Policy;
- PSEAH Policy;
- Complaint Handling Policy;
- Financial Wrongdoing Policy;
- Code of Conduct;
- Whistleblowing procedures.

Types of Incidents That Must Be Reported

Incidents requiring reporting may include, but are not limited to:

- Child safeguarding concerns;
- Sexual exploitation, abuse, or harassment concerns;
- Fraud or financial misconduct;
- Security incidents;

- Workplace injuries or safety incidents;
- Threats or violence;
- Serious misconduct;
- Privacy or data breaches;
- Cybersecurity incidents;
- Operational disruptions;
- Partner misconduct concerns;
- Legal or compliance concerns;
- Reputational concerns;
- Serious community complaints.

Incident Reporting Flow

Step 1 – Incident Identified

An incident, allegation, concern, risk, complaint, or unsafe situation is identified by:

- Staff;
- Volunteers;
- Beneficiaries;
- Community members;
- Partners;
- Contractors;
- Stakeholders.

Examples:

- Safeguarding concern;
- Fraud concern;
- Security threat;
- Serious misconduct;
- Operational incident.

Step 2 – Immediate Safety and Protection Measures

Where immediate risk exists, priority must be given to:

- Protecting affected individuals;

- Preventing further harm;
- Ensuring safety and wellbeing;
- Seeking emergency assistance if required.

Immediate actions may include:

- Removing individuals from danger;
- Contacting emergency services;
- Seeking medical support;
- Separating alleged perpetrators from activities;
- Activating safeguarding or emergency procedures.

Step 3 – Report the Incident Promptly

The incident should be reported as soon as possible to an appropriate BCDC focal person or reporting channel.

Possible reporting channels may include:

- Supervisor or manager;
- Safeguarding Focal Person;
- Executive Team;
- Board representative;
- Complaint handling contact;
- Whistleblower reporting channel.

Reports may be submitted:

- Verbally;
- In writing;
- Through reporting forms;
- Confidentially where appropriate.

Anonymous reporting may also be accepted where feasible.

Step 4 – Initial Documentation and Risk Assessment

The receiving personnel should:

- Record the incident details;
- Assess immediate risks;
- Determine safeguarding or security concerns;

- Identify urgent response needs;
- Maintain confidentiality.

Initial information may include:

- Date and time;
- Persons involved;
- Nature of incident;
- Immediate actions taken;
- Witness information;
- Risk level assessment.

Step 5 – Escalation and Referral

Depending on the seriousness and nature of the incident, the matter may be escalated to:

- Executive management;
- Safeguarding leadership;
- Board representatives;
- External authorities;
- Law enforcement;
- Child protection authorities;
- Medical or psychosocial support providers.

Critical or high-risk incidents should be escalated immediately.

Step 6 – Investigation or Review Process

Where appropriate, BCDC may:

- Conduct an internal review or investigation;
- Coordinate safeguarding responses;
- Seek specialist advice;
- Engage external investigators if required.

Investigations should:

- Be fair and impartial;
- Protect confidentiality;
- Follow survivor-centred approaches;

- Avoid retaliation or victimisation.

Step 7 – Risk Mitigation and Corrective Actions

BCDC may implement corrective actions such as:

- Additional safeguarding measures;
- Staff or volunteer management actions;
- Operational changes;
- Policy or procedural improvements;
- Training and awareness activities;
- Suspension or termination of partnerships or engagements;
- Security or financial control improvements.

Step 8 – Monitoring and Follow-Up

BCDC may:

- Monitor ongoing risks;
- Support affected individuals;
- Review effectiveness of mitigation measures;
- Update the Risk Register where appropriate;
- Document lessons learned.

Step 9 – Closure and Record Keeping

The incident may be formally closed once:

- Appropriate actions have been completed;
- Risks are managed appropriately;
- Documentation is finalised;
- Follow-up actions are completed.

Records should be:

- Stored securely;
- Kept confidential;
- Accessible only to authorised personnel.

BCDC INCIDENT REPORTING AND ESCALATION FLOWCHART

Purpose: To ensure that all incidents, concerns, allegations, or risks are reported promptly, managed appropriately, and escalated to the right level to protect people, reduce risk, and support accountability.

1 INCIDENT IDENTIFIED

An incident, concern, allegation, complaint, or risk is observed or reported by any person.

Examples include:
- Safeguarding concerns (child abuse, sexual exploitation, harassment)
- Fraud or financial misconduct
- Security incidents or threats
- Serious misconduct or policy breaches
- Workplace injury or safety incidents
- Data breaches or privacy concerns
- Operational disruptions

2 IMMEDIATE SAFETY AND PROTECTION

Ensure immediate safety and wellbeing of affected individuals and others.

Take immediate action to:
- Protect the person(s) at risk
- Stop the incident if safe to do so
- Seek medical or emergency help if needed
- Contact emergency services if necessary
- Separate the alleged perpetrator from activities
- Provide initial support to affected person(s)

3 REPORT THE INCIDENT PROMPTLY

Report the incident as soon as possible using an appropriate reporting channel.

Report to one of the following:
- Your supervisor or manager
- Safeguarding Focal Person
- Executive Team member
- Complaint Handling Contact
- Whistleblower reporting channel
- Board representative (if necessary)

Reports may be made:
- Verbally
- In writing
- Electronically
- Anonymously (where possible)

4 INITIAL DOCUMENTATION AND RISK ASSESSMENT

Receiving person records the incident and assesses the immediate risk level.

Document key information:
- Date, time, location
- What happened
- People involved
- Immediate actions taken
- Witnesses (if any)
- Risk level (Low / Moderate / High / Critical)

Maintain:
- Confidentiality
- Sensitivity
- Survivor-centred approach
- Do no harm principle

5 ESCALATION AND REFERRAL

Escalate the incident based on its nature, severity, and risk level.

Escalate to:
- Executive Management
- Safeguarding Leadership
- Board Chair (if critical)
- External Authorities (if required)
- Child Protection Services (if required)
- Law Enforcement (if required)

High and Critical incidents must be escalated immediately.

6 INVESTIGATION / REVIEW

Conduct a fair, impartial, and confidential review or investigation as appropriate.

Actions may include:
- Internal investigation or review
- Seek specialist advice
- Engage external investigator (if required)
- Gather information and evidence
- Interview relevant persons
- Document all steps taken

Principles:
- Fair and impartial
- Protection from retaliation
- Respect confidentiality
- Survivor-centred
- In accordance with policy and legal requirements

7 RESPOND AND TAKE CORRECTIVE ACTIONS

Implement actions to address the incident, reduce risk, and prevent recurrence.

Actions may include:
- Support for affected person(s)
- Disciplinary action (if applicable)
- Strengthen controls and safeguards
- Policy or procedure improvements
- Training and awareness
- Suspension or termination (if required)

Follow organisational policies including:
- Safeguarding Policy
- Code of Conduct
- Whistleblower Policy
- HR Policy
- Financial Wrongdoing Policy

8 MONITORING AND FOLLOW-UP

Monitor the situation and ensure all actions are implemented and effective.

- Monitor ongoing risks
- Review effectiveness of actions
- Provide ongoing support to affected persons
- Update the Risk Register (if relevant)
- Ensure learning and continuous improvement

9 CLOSE AND RECORD KEEPING

Close the incident once all actions are completed and maintain secure records.

Ensure that:
- All actions are completed
- Incident is formally closed
- Records are accurate and complete
- Records are stored securely
- Access is restricted to authorised personnel only
- Retention follows organisational policy and legal requirements

INCIDENT LEVEL GUIDE

LOW
Minimal impact or risk. Manage at operational level.

MODERATE
Incident with noticeable impact. Management attention required.

HIGH
Serious incident with significant impact or risk. Escalate to Executive Management.

CRITICAL
Severe incident with potential for serious harm, legal implications or reputational damage. Immediate escalation to Executive Management and Board.

REPORTING PRINCIPLES

- Protect people and prioritise safety
- Maintain confidentiality
- Be respectful and supportive
- Act fairly and impartially
- Protect reporters from retaliation

IMPORTANT

If you are in immediate danger or a life-threatening situation, call emergency services first.

Then report the incident as soon as it is safe to do so.

BCDC is committed to safeguarding and accountability. All incidents will be managed in accordance with our policies, legal obligations, and ACFID Code of Conduct.

Incident Severity Escalation Guidance

Incident Level	Examples	Escalation Requirement
Low	Minor operational issue	Supervisor review
Moderate	Workplace conflict or moderate operational concern	Management review
High	Serious safeguarding concern, major fraud allegation, serious injury	Executive escalation
Critical	Child abuse allegation, sexual exploitation concern, major security incident, severe fraud	Immediate Executive and Board escalation and external referral where required

Confidentiality and Protection

BCDC is committed to:

- Protecting confidentiality;
- Supporting survivor-centred approaches;
- Preventing retaliation;
- Respecting dignity and privacy;
- Protecting whistleblowers and reporters acting in good faith.

Information relating to incidents should only be shared on a need-to-know basis or where legally required.

Important Principles

All incident responses should be:

- Timely;
- Fair;
- Confidential;
- Survivor-centred where applicable;
- Risk-informed;
- Consistent with safeguarding obligations;
- Respectful of human dignity and rights.

Related Policies and Procedures

This flowchart should be implemented together with:

- Risk Management Policy;
- Child Safeguarding Policy;
- PSEAH Policy;
- Complaint Handling Policy;
- Financial Wrongdoing Policy;
- Code of Conduct;
- Whistleblowing procedures;
- Privacy Policy;
- Human Resources Management Policy.

Review

This Incident Reporting Flowchart should be reviewed periodically and updated where necessary to reflect:

- Organisational learning;
- Changes in operational contexts;
- Safeguarding obligations;
- Legal or regulatory requirements;
- ACFID guidance and sector good practice.

Appendix D – Travel Risk Assessment Template

Burmese Community Development Collaboration (BCDC)

Overseas Travel Risk Assessment Form

Part A – Traveller Information

Item	Details
Full Name	
Position / Role	
Department / Program	
Traveller Type	Staff / Volunteer / Consultant / Contractor / Board Member/Other
Contact Number	
Email Address	
Emergency Contact Person	
Emergency Contact Number	
Supervisor / Manager	

Part B – Travel Details

Item	Details
Purpose of Travel	
Destination(s)	
Country / Region	
Departure Date	
Return Date	
Duration of Travel	
Accommodation Arrangements	
Local Partner / Contact	
Mode of Transport	
Planned Activities	

Part C – Context and Security Assessment

Assessment Area	Details
Security Situation	
Political or Conflict Conditions	
Humanitarian Conditions	
Communication Accessibility	
Health Risks	
Environmental / Climate Risks	
Infrastructure Conditions	
Local Restrictions or Curfews	
Other Contextual Concerns	

Part D – Risk Identification and Assessment

Risk Category	Identified Risk	Likelihood	Impact	Overall Risk Rating	Existing Controls	Additional Mitigation Measures
Security Risk						
Health and Medical Risk						
Safeguarding Risk						
Child Safeguarding Risk						
PSEAH Risk						
Transport Risk						
Communication Risk						
Accommodation Risk						
Environmental Risk						
Legal / Compliance Risk						
Reputational Risk						
Operational Risk						
Other Risks						

Part E – Safeguarding and Protection Checklist

Requirement	Yes	No	Comments
Safeguarding induction completed			
PSEAH awareness completed			
Traveller understands reporting obligations			
Traveller understands Code of Conduct obligations			
Emergency contacts confirmed			
Local safeguarding concerns reviewed			
Appropriate supervision arrangements confirmed			
Partner safeguarding systems reviewed			

Part F – Insurance and Medical Considerations

Item	Details
Travel Insurance Arranged	
Insurance Provider	
Coverage Period	
Relevant Medical Conditions	
Medication Requirements	
Vaccinations Required / Completed	
Access to Medical Facilities	
Emergency Medical Plan	

Part G – Emergency and Communication Planning

Item	Details
Primary Communication Method	
Secondary Communication Method	
Local Emergency Contacts	
Embassy / Consular Contact	
Emergency Evacuation Considerations	
Safe Accommodation Confirmed	
Incident Reporting Procedure Explained	
Emergency Escalation Procedure Confirmed	

Part H – Risk Assessment Summary

Assessment Item	Summary
Overall Risk Level	Low / Moderate / High / Critical
Is Travel Recommended?	Yes / No
Conditions or Restrictions	
Additional Safety Requirements	
Monitoring Arrangements	
Escalation Requirements	

Part I – Traveller Declaration

I confirm that:

- The information provided is accurate;
- I understand the identified risks;
- I will comply with BCDC policies and procedures;
- I understand safeguarding, security, and reporting obligations;
- I will immediately report incidents, emergencies, or changes in circumstances.

Name	Signature	Date

Part J – Supervisor / Manager Approval

Name	Position	Signature	Date

Part K – Executive Approval (For High-Risk Travel)

Name	Position	Signature	Date

Appendix E – Due Diligence Checklist

Burmese Community Development Collaboration (BCDC)

Partner Due Diligence Checklist

Part A – Organisation Information

Item	Details
Organisation Name	
Country / Location	
Type of Organisation	
Date of Assessment	
Assessed By	
Contact Person	
Contact Details	
Website / Social Media	
Proposed Partnership / Activity	

Part B – Governance and Organisational Structure

Assessment Item	Yes	No	Comments / Evidence
Organisation has a governing body or leadership structure			
Organisation has a written constitution or governing document			
Roles and responsibilities are clearly defined			
Organisation demonstrates accountability mechanisms			
Organisation maintains organisational records			
Organisation has operational policies and procedures			
Organisation has conflict of interest procedures			

Part C – Safeguarding and PSEAH

Assessment Item	Yes	No	Comments / Evidence
Organisation has a Child Safeguarding Policy			
Organisation has a PSEAH Policy or procedures			
Staff/volunteers receive safeguarding awareness			
Safeguarding reporting procedures exist			
Complaints mechanisms are available			
Organisation demonstrates commitment to safeguarding			
Safeguarding focal person identified			

Part D – Financial Management and Accountability

Assessment Item	Yes	No	Comments / Evidence
Organisation maintains financial records			
Financial approval procedures exist			
Budget monitoring systems exist			
Organisation has banking arrangements			
Financial reporting mechanisms exist			
Organisation demonstrates financial accountability			
Fraud prevention or financial wrongdoing measures exist			

Part E – Legal and Compliance Review

Assessment Item	Yes	No	Comments / Evidence
Organisation is legally registered where applicable			
Organisation complies with local laws and regulations			
No known serious legal or compliance concerns identified			
Organisation demonstrates ethical operational conduct			
Privacy and confidentiality measures exist			

Part F – Sanctions and Prohibited Entities Screening

Screening Requirement	Completed	Comments / Findings
DFAT Consolidated Sanctions List checked		
Australian terrorist organisations list checked		
Publicly available adverse media reviewed		
No prohibited entities concerns identified		
No sanctions concerns identified		

Part G – Operational and Program Capacity

Assessment Item	Yes	No	Comments / Evidence
Organisation has experience relevant to proposed activities			
Organisation has sufficient staffing or volunteer capacity			
Organisation has operational systems in place			
Organisation demonstrates community engagement			
Monitoring or reporting systems exist			
Organisation demonstrates reliability and responsiveness			

Part H – Security and Contextual Risks

Assessment Item	Yes	No	Comments / Evidence
Security risks reviewed			
Political or conflict-related concerns reviewed			
Operational environment assessed			
Travel or access limitations identified			
Safeguarding vulnerabilities identified			
Mitigation measures considered			

Part I – Reputation and Community Standing

Assessment Item	Yes	No	Comments / Evidence
Organisation has positive community reputation			
No significant reputational concerns identified			
Community references or recommendations obtained			
Organisation aligns with BCDC values and principles			

Part J – Risk Assessment Summary

Assessment Area	Summary
Overall Risk Level	Low / Moderate / High / Critical
Key Risks Identified	
Mitigation Measures Required	
Additional Conditions or Restrictions	
Is Partnership Recommended?	Yes / No
Monitoring Requirements	

Part K – Final Recommendation

Recommendation	Tick
Partnership Recommended	
Partnership Recommended with Conditions	
Further Review Required	
Partnership Not Recommended	

Comments:

Part L – Approval

Assessor

Name	Position	Signature	Date

Management Approval

Name	Position	Signature	Date

Executive / Board Approval

Name	Position	Signature	Date

Appendix F – Emergency Contact Procedures Template

Burmese Community Development Collaboration (BCDC)

Emergency Response and Contact Procedures Form

Part A – Emergency Incident Information

Item	Details
Date of Incident	
Time of Incident	
Location	
Type of Emergency	Medical / Safeguarding / Security / Travel / Cybersecurity / Natural Disaster / Other
Person Reporting Incident	
Position / Role	
Contact Number	
Persons Affected	
Immediate Risk Level	Low / Moderate / High / Critical

Part B – Immediate Safety Actions Taken

Immediate Response Action	Completed	Comments
Emergency services contacted		
Medical assistance provided		
Individuals moved to safe location		
Safeguarding protection measures implemented		
Supervisor notified		
Emergency contacts informed		
Security advice followed		
Incident documented		

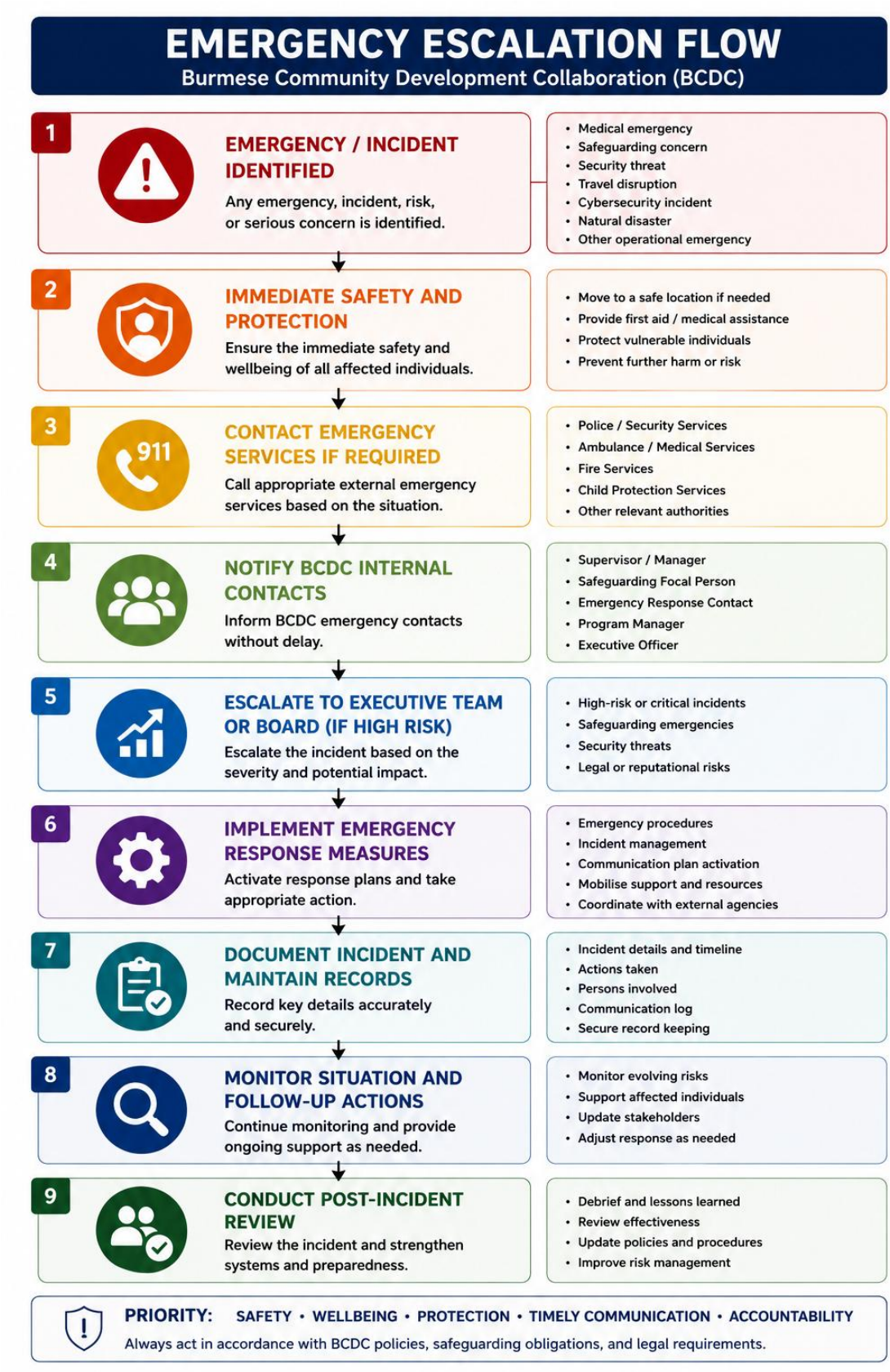
Part C – Internal Emergency Contact List

Position / Role	Name	Contact Number	Contacted?	Time Contacted
Executive Officer				
Safeguarding Focal Person				
Board Representative				
Program Manager				
Finance Officer				
Volunteer Coordinator				
Emergency Response Contact				

Part D – External Emergency Contacts

Organisation / Service	Contact Number	Contacted?	Time Contacted	Notes
Police / Emergency Services				
Ambulance / Medical Services				
Hospital / Clinic				
Child Protection Authority				
Embassy / Consular Contact				
Insurance Emergency Assistance				
Local Security Contact				
Legal Assistance Contact				

Part E – Emergency Escalation Flow



Part F – Emergency Assessment Summary

Assessment Area	Details
Current Situation Summary	
Immediate Threats Identified	
Safeguarding Concerns	
Medical Concerns	
Security Concerns	
Operational Impact	
Additional Support Required	
Ongoing Monitoring Required	

Part G – Communication and Follow-Up

Follow-Up Requirement	Completed	Comments
Affected individuals supported		
Relevant stakeholders informed		
Safeguarding procedures followed		
Risk Register updated		
Incident report completed		
Additional mitigation measures implemented		
Lessons learned reviewed		

Part H – Final Review and Closure

Item	Details
Final Risk Status	
Was further escalation required?	
Corrective actions completed?	
Date incident closed	

Reviewed By	
Position	
Signature	
Date	

Confidentiality Notice

All emergency-related information must be:

- Treated confidentially;
- Shared only on a need-to-know basis;
- Stored securely;
- Managed in accordance with BCDC safeguarding, privacy, and incident management obligations.

Related Policies and Procedures

This template should be used together with:

- Risk Management Policy;
- Incident Reporting Procedures;
- Child Safeguarding Policy;
- PSEAH Policy;
- Complaint Handling Policy;
- Financial Wrongdoing Policy;
- Travel Risk Assessment procedures;
- Business Continuity procedures.

Appendix G – Partner Risk Screening Checklist

Burmese Community Development Collaboration (BCDC)

Partner Risk Screening Checklist

Part A – Partner Information

Item	Details
Organisation Name	
Country / Region	
Organisation Type	
Date of Screening	
Assessed By	
Main Contact Person	
Contact Number	
Email Address	
Website / Social Media	
Proposed Partnership Activity	

Part B – Organisational Background Review

Assessment Item	Yes	No	Comments / Evidence
Organisation identity verified			
Organisation has operational history			
Organisation has identifiable leadership structure			
Organisation has governing document or constitution			
Organisation demonstrates community legitimacy			
Organisation has relevant operational experience			
Organisation has clear contact information			

Part C – Governance and Accountability Screening

Assessment Item	Yes	No	Comments / Evidence
Governance structure reviewed			
Roles and responsibilities are defined			
Accountability mechanisms identified			
Financial oversight arrangements exist			
Conflict of interest measures exist			
Complaint handling mechanisms exist			
Organisational policies reviewed			

Part D – Safeguarding and PSEAH Screening

Assessment Item	Yes	No	Comments / Evidence
Child Safeguarding Policy exists			
PSEAH Policy or procedures exist			
Safeguarding focal person identified			
Safeguarding reporting procedures exist			
Complaints mechanisms are accessible			
Safeguarding awareness or training conducted			
No known safeguarding concerns identified			

Part E – Financial and Operational Screening

Assessment Item	Yes	No	Comments / Evidence
Financial records maintained			
Banking arrangements verified			
Financial approval procedures exist			
Budget management systems exist			
Operational capacity reviewed			
Staffing or volunteer capacity sufficient			
Program delivery systems identified			

Part F – Legal and Compliance Screening

Assessment Item	Yes	No	Comments / Evidence
Organisation legally registered where applicable			
Compliance concerns identified			
Organisation demonstrates ethical conduct			
Privacy/confidentiality procedures exist			
No known serious legal concerns identified			

Part G – Sanctions and Prohibited Entities Screening

Screening Requirement	Completed	Findings / Comments
DFAT Consolidated Sanctions List checked		
Australian terrorist organisations list checked		
Public adverse media search conducted		
No sanctions concerns identified		
No prohibited entities concerns identified		
No links to terrorism financing identified		

Part H – Security and Contextual Risk Screening

Assessment Item	Yes	No	Comments / Evidence
Security risks reviewed			
Conflict or political risks assessed			
Operational environment reviewed			
Access or travel restrictions identified			
Community vulnerabilities considered			
Safeguarding risks considered			

Part I – Reputation and Community Standing

Assessment Item	Yes	No	Comments / Evidence
Community references obtained			
Organisation demonstrates positive reputation			
No major reputational concerns identified			
Alignment with BCDC values confirmed			
Community trust or engagement evident			

Part J – Risk Assessment Summary

Assessment Area	Summary
Overall Risk Level	Low / Moderate / High / Critical
Key Risks Identified	
Additional Controls Required	
Monitoring Requirements	
Partnership Conditions Required	
Is Partnership Recommended?	Yes / No

Part K – Final Screening Recommendation

Recommendation	Tick
Approved	
Approved with Conditions	
Further Review Required	
Not Approved	

Comments:

Part L – Approval and Authorisation

Assessor

Name	Position	Signature	Date

Management Review

Name	Position	Signature	Date

Executive / Board Approval

Name	Position	Signature	Date

Burmese Community Development Collaboration (BCDC)

Safeguarding Risk Assessment Guide

Purpose

This Safeguarding Risk Assessment Guide supports BCDC personnel, volunteers, consultants, contractors, partner organisations, and program teams in identifying, assessing, managing, and mitigating safeguarding-related risks across all organisational activities.

This guide is intended to:

- Strengthen safeguarding practices;
- Prevent harm, abuse, exploitation, and misconduct;
- Support child safeguarding and PSEAH obligations;
- Promote safe organisational environments;
- Integrate safeguarding into operational planning and risk management processes.

This guide should be used together with:

- Child Safeguarding Policy;
- PSEAH Policy;
- Risk Management Policy;
- Code of Conduct;
- Complaint Handling Policy;
- Incident Reporting Procedures.

Part A – Activity / Program Information

Item	Details
Program / Activity Name	
Location	
Date of Assessment	
Conducted By	
Department / Program Team	
Partner Organisation (if applicable)	
Type of Activity	
Participants Involved	

Part B – Safeguarding Context Assessment

Assessment Area	Details
Vulnerable Groups Involved	
Children Involved?	Yes / No
Women or At-Risk Groups Involved?	Yes / No
Community Context Considerations	
Security / Conflict Conditions	
Cultural or Language Considerations	
Accessibility or Inclusion Considerations	
Previous Safeguarding Concerns Identified?	

Part C – Safeguarding Risk Identification

Risk Area	Potential Safeguarding Risk	Persons Potentially Affected	Existing Controls	Additional Controls Required
Child Safeguarding				
PSEAH Risk				
Unsafe Staff / Volunteer Conduct				
Community Interaction Risks				
Travel or Transport Risks				
Online or Digital Risks				
Privacy and Confidentiality Risks				
Partner-Related Risks				
Security-Related Risks				
Communication Risks				
Inclusion and Accessibility Risks				
Other Safeguarding Risks				

Part D – Safeguarding Risk Rating

Identified Risk	Likelihood	Impact	Overall Risk Rating	Mitigation Priority
Example - Children may become separated from guardians during community activities	*Possible*	*Major*	*High*	*High Priority*

Part E – Safeguarding Controls Checklist

Safeguarding Requirement	Yes	No	Comments
Staff/volunteers received safeguarding induction			
PSEAH awareness completed			
Code of Conduct signed			
Child safeguarding procedures reviewed			
Reporting procedures explained			
Safeguarding focal person identified			
Complaints mechanisms accessible			
Appropriate supervision arrangements exist			
Risk mitigation measures implemented			
Privacy and confidentiality protections in place			

Part F – Partner Safeguarding Review (if applicable)

Assessment Item	Yes	No	Comments
Partner has safeguarding policy			
Partner has PSEAH procedures			
Partner understands reporting obligations			
Partner safeguarding focal person identified			
Partner complaints mechanisms reviewed			
No known safeguarding concerns identified			

Part G – Safeguarding Mitigation Action Plan

Action Required	Responsible Person	Timeline	Status
Example ***Conduct safeguarding refresher briefing for all volunteers and staff before the activity***	***Safeguarding Focal Person***	***Before activity commencement***	***Completed***

Part H – Overall Safeguarding Assessment Summary

Assessment Area	Summary
Overall Safeguarding Risk Level	Low / Moderate / High / Critical
Key Safeguarding Risks Identified	
Additional Safeguarding Controls Required	
Ongoing Monitoring Requirements	
Is Activity Recommended?	Yes / No
Conditions or Restrictions Required	

Part I – Approval and Review

Assessor

Name	Position	Signature	Date

Management Review

Name	Position	Signature	Date

Safeguarding Focal Person Review

Name	Position	Signature	Date

Safeguarding Risk Assessment Guidance

Examples of Safeguarding Risks

Safeguarding risks may include:

- Harm to children or vulnerable individuals;
- Sexual exploitation, abuse, or harassment;
- Inappropriate staff or volunteer behaviour;
- Unsafe community engagement practices;
- Lack of reporting mechanisms;
- Privacy or confidentiality breaches;
- Unsafe online communication;
- Security risks affecting vulnerable populations.

High-Risk Activities May Include

- Activities involving children;
- Community outreach in unstable environments;
- Cross-border or conflict-area activities;
- Emergency humanitarian responses;
- Home visits or direct beneficiary engagement;
- Activities involving overnight travel;
- Digital engagement involving vulnerable groups.

Important Principles

All safeguarding assessments should:

- Prioritise prevention of harm;
- Follow survivor-centred approaches;
- Respect dignity and confidentiality;
- Consider power imbalances and vulnerabilities;
- Integrate inclusion and accessibility considerations;
- Promote accountability and safe reporting.

Related Policies and Procedures

This guide should be used together with:

- Child Safeguarding Policy;
- PSEAH Policy;
- Risk Management Policy;
- Complaint Handling Policy;
- Incident Reporting Procedures;
- Code of Conduct;
- Human Resources Management Policy;
- Volunteer Management procedures.

Review

This Safeguarding Risk Assessment Guide should be reviewed periodically to ensure alignment with:

- Organisational safeguarding obligations;
- Operational contexts;
- ACFID guidance and standards;
- Emerging safeguarding risks and sector good practice.

Appendix I – Risk Monitoring and Review Schedule

Burmese Community Development Collaboration (BCDC)

Risk Monitoring and Review Schedule

Purpose

This Risk Monitoring and Review Schedule is designed to support ongoing monitoring, review, evaluation, and improvement of BCDC's organisational risk management systems, safeguarding measures, operational controls, and governance processes.

The schedule supports:

- Continuous monitoring of organisational risks;
- Timely review of mitigation measures;
- Governance oversight and accountability;
- Safeguarding and compliance monitoring;
- Organisational learning and continuous improvement;
- Early identification of emerging risks.

This schedule should be used together with:

- Risk Register;
- Incident Reporting Procedures;
- Safeguarding systems;
- Due Diligence procedures;
- Monitoring and Evaluation systems.

Risk Monitoring and Review Schedule Table

Risk Area / System	Monitoring Activity	Responsible Person / Team	Frequency	Monitoring Method	Reporting / Review Mechanism	Status / Comments
Organisational Risk Register	Review and update identified organisational risks	Executive Team / Management	Quarterly	Risk Register review meetings	Management and Board review	
Safeguarding Risks	Monitor safeguarding incidents, complaints, and mitigation measures	Safeguarding Focal Person	Monthly	Incident review and safeguarding monitoring	Safeguarding review meetings	
Child Safeguarding Systems	Review child safeguarding compliance and procedures	Safeguarding Team	Quarterly	Safeguarding assessments and reporting	Management review	
PSEAH Risks	Monitor PSEAH prevention and reporting mechanisms	Safeguarding Focal Person	Quarterly	Incident monitoring and awareness review	Executive review	
Financial Risks	Monitor financial controls, approvals, and reporting	Finance Officer	Monthly	Financial reconciliation and review	Financial reporting meetings	
Fraud and Corruption Risks	Review fraud prevention controls and financial integrity systems	Finance Officer / Executive Team	Quarterly	Internal financial review	Board and management oversight	
Operational Risks	Review operational challenges and implementation risks	Program Team	Monthly	Program monitoring meetings	Program review meetings	
Human Resource Risks	Monitor staffing, wellbeing, and workplace concerns	HR Focal Person	Quarterly	Staff review and supervision	Management review	
Volunteer Management Risks	Review volunteer safeguarding and supervision arrangements	Volunteer Coordinator	Quarterly	Volunteer monitoring and feedback	Program management review	
Health and Safety Risks	Monitor workplace and activity safety concerns	Management Team	Quarterly	Safety assessments and incident review	Internal review meetings	
Security Risks	Monitor conflict, political, and security developments	Executive Team	Monthly	Context and security monitoring	Security briefings and management review	

Overseas Travel Risks	Review approved travel activities and travel-related incidents	Program Manager	Before and after travel	Travel risk assessment review	Executive review	
Partnership Risks	Review partner safeguarding, governance, and operational compliance	Program Manager / Partnership Team	Quarterly	Partner monitoring and communication	Partnership review meetings	
Legal and Compliance Risks	Review compliance with policies, legal obligations, and ACFID requirements	Executive Team / Board	Quarterly	Compliance review and policy assessment	Governance meetings	
Privacy and Data Protection Risks	Monitor confidentiality and data protection practices	Administration Team	Quarterly	System and records review	Internal compliance review	
Cybersecurity Risks	Review cybersecurity risks and system protections	Administration / IT Support	Quarterly	System monitoring and access review	Management review	
Reputational Risks	Monitor complaints, public concerns, and stakeholder feedback	Executive Team	Quarterly	Stakeholder feedback review	Governance and communication review	
Environmental and Climate Risks	Review environmental and climate-related operational risks	Program Team	Annually	Operational and environmental assessment	Program review meetings	
Community Relations Risks	Monitor community engagement and stakeholder concerns	Community Engagement Team	Quarterly	Community feedback and consultation	Program review meetings	
Program Delivery Risks	Review program implementation, outcomes, and operational effectiveness	Program Team	Monthly	PMEL review and program monitoring	Program management meetings	
Emergency and Crisis Preparedness	Review emergency response and operational continuity arrangements	Executive Team	Annually	Emergency preparedness review	Board and management review	

Monitoring Guidance

Monitoring Responsibilities

Responsible personnel should:

- Monitor assigned risks regularly;
- Review effectiveness of mitigation measures;
- Escalate significant or emerging risks;
- Maintain documentation and records;
- Support continuous improvement processes.

Escalation Requirements

High-risk or critical-risk issues should be:

- Escalated promptly to management;
- Recorded in the Risk Register;
- Reviewed by Executive leadership or the Board where appropriate;
- Subject to additional monitoring and mitigation measures.

Review Triggers

Risk reviews may also be conducted when:

- Serious incidents occur;

- Safeguarding concerns arise;
- Operational contexts change significantly;
- New programs or partnerships are introduced;
- Humanitarian or security conditions deteriorate;
- Legal or compliance requirements change.

Continuous Improvement

BCDC recognises that risk management is an ongoing process requiring:

- Regular monitoring;
- Reflection and learning;
- Policy review;
- Operational adaptation;
- Stakeholder feedback;
- Strengthening of systems and controls.

Findings from monitoring and review activities may inform:

- Policy updates;
- Training improvements;
- Operational adjustments;
- Safeguarding strengthening measures;

- Governance and accountability improvements.

Documentation and Record Keeping

Monitoring and review records should:

- Be documented appropriately;
- Be stored securely;
- Remain accessible to authorised personnel;
- Support organisational accountability and audit processes.

Sensitive safeguarding or security-related information must be managed confidentially.

Related Policies and Procedures

This schedule should be used together with:

- Risk Management Policy;
- Risk Register;
- Safeguarding Policies;
- PSEAH Policy;
- Incident Reporting Procedures;
- Complaint Handling Policy;
- PMEL systems;
- Due Diligence procedures;

- Emergency and Crisis Management procedures.

Review

This Risk Monitoring and Review Schedule should be reviewed periodically to ensure alignment with:

- Organisational needs;
- Operational contexts;
- Safeguarding obligations;
- ACFID guidance and standards;
- Emerging risks and sector good practice.